MIT-NED-EDF-2000-01

Incident Management via Probabilistic Safety Assessment and Formal Decision-Making Techniques for Nuclear Power Plants

Phase 1 Final Report

"The Use of PSA to Support NPP Accident Management"

by

Emanuele Borgonovo, Curtis Smith, and George Apostolakis
Massachusetts Institute of Technology

February 2000

ABSTRACT

This report provides details for the research for Phase 1 of the project “Use of PSA to Support NPP Accident Management." For this work, we assessed the issues facing the application of PSA and formal decision-making methods to the topics of incident management and operational decision-making. We focused on the PSA capability of modeling an actual sequence, with particular attention to the issues of sequential decisions and the time-flow of the events. We analyzed two case studies: the Davis-Besse Loss of Main Feedwater Event and the Catawba Loss of Offsite Power event. In this final report we also analyzed the decision making aspects of the last phase of the Catawba event, where operational and managerial decisions play a relevant role. One of the outcomes of the research is that PSA seems to be a capable tool of prioritizing and postulating decision alternatives during an incident as well as in operation management. Thus, PSA insights coupled with formal decision-making techniques (such as influence diagrams or decision trees) provide a robust framework from which an incident and/or operation management system could be constructed.

CONTENTS

"The Use of PSA to support NPP Incident Management"

1. INTRODUCTION

This report provides the results of the project: "The Use of PSA to support NPP Accident Management". In the first phase of the project (Task 1), we analyzed and reviewed international activities in the area of Accident Management with the purpose of exploring potential candidate tools and methodologies to integrate the use of probabilistic safety analysis (PSA) in decision-making during an off-normal or “incident” situation (pre-core damage). Those results are documented in a separate report.

One of the main results of Task 1 has been that accident management must be considered a "sequential decision problem under uncertainty." Organizational issues, psychological issues and human performance are an important part of the problem (Dougherty, 1992), as proved by ongoing work in the area performed by engineers in close contact with psychologists (Svenson, 1998; Holmberg et al., 1999).

An incident management methodology that copes with the problem as thoroughly as possible must give proper consideration to many aspects (e.g., human performance, equipment condition, timing considerations). As a result of Task 1, it appears that methodologies based on an unstructured use of expert judgment or concerning only the physics of an accident sequence do not tackle the problem in its completeness. Instead, PSA accompanied with the use of Influence Diagrams (ID) and Decision Trees (DT) proposes itself as the most suitable tool to an integrated approach to the problem of incident management.

A similar approach (of a blended PSA and ID/DT method) has been taken by a couple of reearch teams. (Jae , Apostolakis et al., 1992; Jae, Apostolakis 1993; Catton and Kastenberg, 1998) Note though that all of these earlier works focused only on post-core damage (CD) situations. As it was noted in the Task 1 report of this project, problems and issues that arise after CD may be quite different from those that arise in a pre-CD, off-normal situation. For example, in the case of post-CD accidents, the decision maker will be concerned only with "safety" as an objective. In the case of pre-CD incidents, at least at the beginning of the scenario, the decision maker (probably the shift supervisor at the plant) will be concerned at first with avoiding plant actions that result in economic impacts (e.g., reactor or turbine trip). Furthermore, in the first case (post-CD), uncertainties are dominated by those deriving from the physics of the problem (e.g., how will the corium behave?) while in the second case the plant configuration and operator actions dominate the scene.

The second phase of the project has resulted in the analysis of two precursors[1] with the purpose of gaining insight on the following aspects:

S Peculiarities and issues of the decision-making phase in a pre-CD situation

S Applicability of the PSA with respect to its potential use as a modeling tool and assistance on related decision-making issues

S Integration of PSA and IDs and DTs as a modeling tool during incident management.

While the current research focus has been on relatively short-duration events, the methods and insights gained from the work should be applicable to longer-period events (e.g., operational decision-making).

In Section 2, we describe the two case studies that are utilized. The first case refers to the so called "Davis-Besse event" (from the name of the plant where it happened). In 1985, a loss of main feedwater (MFW), accompanied by human error to start the auxiliary feedwater (AFW) system brought the plant into a risky off-normal situation. This situation almost led the crew to go to “feed-and-bleed” cooling. The entire event duration lasted just short of twenty minutes.

The second case study refers to a loss of offsite power at the Catawba nuclear power plant (NPP). This event was complicated by the fact that at the time that offsite power was lost, one of two emergency diesel generators was unavailable due to maintenance. Consequently, the plant suffered a partial station blackout. The entire event duration lasted over 70 hours.

In Section 3, we discuss issues and potentialities the analyst faces in applying PSA to the analysis of an accident sequence. As we demonstrate, the PSA model is capable of pointing out the most important decisions (or decision alternatives). This information, derived from PSA, can be given to the decision-maker (e.g., the shift supervisor) to prevent going close to core damage. Alternatively, the PSA information may assist in “recovering” from a situation that is approaching core damage. Results of the analysis of the two case studies will be presented.

[1] By “precursor” we mean any off-normal situation that could occur at a NPP that approaches but does not reach core damage.

Then, in Section 4, we discuss the problem of a model for the evaluation of decisions during an incident. We demonstrate that in our cases, the analysis could be facilitated by the use of IDs and DTs. Results from the formal decision-making process will be presented for the two case studies.

Lastly, in Section 5 we will illustrate and discuss the conclusions of our work.

2. CASE STUDIES

2.1 General Overview

In order to investigate potential methods of incident management using PSA and formal decision-making techniques, two case studies were identified. The first case study was selected to be the loss of feedwater incident that happened at the Davis-Besse NPP in June of 1985. The second case study was selected to be the loss of offsite power incident that happened at the Catawba NPP in February of 1996. These two events were selected for several reasons, namely:

S The incidents represented complex scenarios that took a NPP somewhat close to a potential core-damage event.

S Relevant information (e.g., timing, operator actions) for each event is available since the events were evaluated by the U.S. Nuclear Regulatory Commission.

S The events represent extremes in timing considerations during the incident. The Davis-Besse event represents a short duration event (the time from the start of the event to loss of all feedwater was approximately 6 minutes). Conversely, the Catawba event represents a loss of offsite power event that lasted over 36 hours (the time to completely restore offsite power was over 36 hours).

S The incidents both represent a relevant initiating event scenario at a NPP.

S Both incidents occurred at a pressurized water reactor NPP.

The Davis-Besse NPP is owned by the Toledo Edison Company and is located in Ohio. The reactor is rated at 2772 Mwt and 906 MWe (net). It is a 2-loop PWR built by Babcock & Wilcox. It begun commercial operation in July of 1978. The plant has two steam generators and two main feedwater (MFW) pumps. These two pumps are steam driven, which, consequently, implies that if the steam generators trip (i.e., are isolated) and steam is not available to the MFW pumps, it will take approximately 30 minutes to restore steam to these pumps. A startup feedwater pump is also available to provide some flow to the steam generators in the case that all feedwater is lost.

The Catawba NPP is owned by Duke Power Company and is located in South Carolina. The reactor is rated at 3411 MWt and 1129 MWe (net). It is a 4-loop PWR built by Westinghouse. It began commercial operation in August of 1986. The plant has four steam generators and three main feedwater pumps. The plant has two emergency diesel generators.

2.2 Davis-Besse Loss of Feedwater Scenario Description

At 1:35 in the morning, while the plant was at 90% power, the first of two steam-driven MFW pumps experienced an over-speed event, causing the pump to stop. Shortly after (approximately 1/2 min), the main steam isolation valves (MSIV) closed, which impacted the other pump, MFWP-2. At this same time, the plant scrammed. Over the course of the next 4-1/2 min, MFWP-2 coasts down, providing the sole source of feedwater flow to the steam generators.

With the feedwater tapering off, it would only be a matter of minutes before the auxiliary feedwater (AFW) system would actuate automatically based upon a signal from the plant safety control system. But, at about six minutes after the loss of the MFWP-1, the secondary-side reactor operator (RO2) received permission from the person in charge of the control room, the shift supervisor (SRO1), to actuate AFW before the safety control system performs the actuation. This step was requested on the part of RO2 in order to preserve water inventory in the steam generators. Unfortunately, after going to the control panel (in the control room) to actuate the system, the operator incorrectly *isolated* the AFW system. At this point (six minutes into the scenario), the plant had lost all feedwater to both steam generators.

After 1/2 min, the AFW pumps tripped due to the system isolation. The operators are now aware that a very serious situation exists. Two-and-a-half minutes later, the steam generators boiled (essentially) dry. A total time of only nine minutes have elapsed from the loss of one MFWP to boiling both steam generators dry.

At the time nine minutes, SRO1 sent two groups of two equipment operators into the plant to restore the AFW system. They had to perform two actions: (1) un-isolate the AFW isolation valves (which are locked valves in locked rooms three levels below the control room) and (2) un-trip the AFWPs (via restoring tripped throttle valves to their original position). At this same time, the auxiliary shift supervisor (SRO2) decided to help gain time by attempting to start a motor-driven startup feedwater pump (this is a small pump used only when the plant is below 40% power). This pump, if started, would provide some water to the steam generators, but the amount of water would not be enough to completely cool the primary system. SRO2 was successful in starting the startup feedwater pump in only four minute, an action that was estimated to take between 15 and 20 minutes.

After a total of 16 minutes from the start of the scenario, and after the steam generators have been “dry” for five minutes, both SRO2 and RO2 suggested to SRO1 that feed-and-bleed (F&B) cooling be initiated. The plant technical specification called for F&B cooling to be started at this point. The SRO1 decides to continue attempts to restore AFW even though he understands that if he waits too long, there comes a point where even F&B cooling will not be able to adequately cool the primary system (and possibly result in melting core fuel). But, after another three minutes, the AFWPs are realigned and are successfully started, thereby injecting cooling water into the steam generators. The AFW system continues to operate, thereby ending the scenario.

The scenario is represented by the sequence of events shown below:

0.0 min	MFW1 pump trip (the reactor and turbine trip at t = 30 sec)
0.5 min	MSIV closed (MFW2 pump coast down over 4.5 min.)
6.0 min	RO2 incorrectly trips SFRCS (which isolates AFW)
6.5 min	AFW pumps trip on overspeed
7.0 min	RO2 finds error of AFW isolation
7.0 min	RO1 resets SFRCS. Since AFW isolated, it does not reset
7.5 min	RO1 open press. spray, RCS press. decreases
9.0 min	Both steam generators boil dry
9.0 min	RO1 and SRO1 send equipment operators to restore AFW
9.0 min	SRO2 decides to use startup feedwater pump (“heroic” action)
11.0 min	RO2 sent RO1 to reset startup feedwater pump, primary PORV opens
16.0 min	RO2 and SRO2 recommend feed-and-bleed be initiated
16.5 min	RO2 starts the startup feedwater pump into steam generator 1
18-20 min	AFW pumps align and begin to function

2.3 Catawba Loss of Offsite Power Description

At 12:31 in the afternoon, while the plant was at 100% power, ground faults on both main transformers started a loss of offsite power (LOOP). The reactor scrammed very shortly after the LOOP. The plant has two on-site emergency diesel generators (EDGs), EDG-A and EDG-B. Very shortly after the reactor scram, EDG-A started automatically. EDG-B was out of service at the time of the LOOP.

Five minutes after the LOOP, the operators closed the main steam isolation valve. Two minutes later, safety injection (SI) occurred due to low steam pressure in steam generator (SG) A. Eleven minutes later, the reactor coolant system pressurizer power-operated relief valve (PORV) began to open and close. After another 23 minutes, the pressurizer went solid. This situation led to a rupture of the pressurizer rupture disc ten minutes later. It wasn’t until approximately 6 hours later that a steam bubble was restored in the pressurizer.

Also, around this time frame (4 hr 11 min), the operators noted a leak in the penetration room from the turbine-driven (TD) auxiliary feedwater (AFW) pump. One hour and 18 min later, the TDAFW was isolated.

Repairs on EDG-B were underway at the time of the LOOP. The EDG-B was restored approximately three hours after the LOOP. Partial offsite power was restored to the “B” busses approximately 5-1/2 hours after the LOOP. Additional partial offsite power sources were available to the “A” busses approximately 7-1/2 hours after the LOOP. Full restoration of offsite power was realized around 36 hours after the LOOP. The plant was moved to a hot shutdown state at 975 minutes and then later to a cold shutdown state. Note that the full text of the LER event is found in Appendix A of this report.

The scenario is represented by the sequence of events shown below:

0 min	LOOP with unavailability of diesel generator B
5 min	Close MSIV
7 min	SI started
18 min	PORV begin cycling
41 min	Pressurizer is solid
51 min	Pressurizer rupture disc ruptures
180 min	EDG-B restored to service
251 min	Leak from TD AFW pump
329 min	TD AFW pump isolated
330 min	Partial restoration of off-site power to “B” busses
470 min	Partial restoration of off-site power to “A” busses
975 min	Hot Shutdown
1712 min	Cold Shutdown
2160 min	Full restoration of off-site power

3. PSA ANALYSIS METHODS

3.1 PSA Analysis for Davis-Besse Loss of Feedwater Scenario

To explore the characteristics of decision-making during incidents at NPPs, we first explored the Davis-Besse loss of feedwater event using a PSA model. While the actual Davis-Besse plant model was not available for this exploratory analysis, another PWR plant model was utilized. This other model was the Surry NUREG-1150 model developed for the U.S. Nuclear Regulatory Commission as part of the NPP Severe Accident Risk program in the 1980's and early 1990's (Bertucio and Julius, 1990). This model was used in conjunction with the SAPHIRE PSA software (Smith, Thatcher, and Knudsen, 1998). For actual incident investigation, it would be a requirement that the actual plant PSA be used for any analysis.

The first step of the PSA analysis for the loss of feedwater event was to decompose the sequence of events into blocks of times where the plant was in a particular *configuration*. Thus, we are discretizing the plant state into time bins, where like time bins are grouped together into a single bin. This step is similar to that used by so-called “risk monitors” in use a some NPPs today. For the loss of feedwater event, there was a total of eight configurations over the course of the event. These configurations are summarized below:

Configuration	Time	Description
1	0.0 min	The nominal plant state
2	0.0 min	Loss of MFW1 pump
3	0.5 min	Plant trip and MSIV closed
4	5.0 min	Complete loss of MFW system and plant in tripped state
5	6.0 min	Loss of MFW and isolation of AFW
6	9.0 min	Both steam generators boil dry, still no MFW or AFW
7	16.5 min	Startup feedwater pump injects into steam generator 1, still no MFW or AFW
8	19.0 min	AFW pumps align and begin to function

After the discretization and identification of each plant state over time, we must then evaluate each state using the PSA model. To perform this step, the plant state during a particular configuration must be “mapped” into the PSA. This mapping process requires the identification of specific basic events in the PSA that are impacted in any way by the component degradations or initiating events that occur at the start of the configuration. Since the Surry PSA has over 1,100 basic events, the mapping process may be difficult and time-consuming. Fortunately, most U.S. PSA models utilize a somewhat consistent naming nomenclature on the basic events. This nomenclature permits the analyst to focus on those basic events of interest since similar events are grouped together, generally by system type.

We have identified each of the relevant basic events for each of the configurations for the loss of feedwater incident. These events are shown in Table 1. Within Table 1 are each configuration, the time that the configuration began during the scenario, and the PSA events of interest. Note that, for this particular scenario, we did not have to consider adjustments to common-cause failures (e.g., common-cause failure of two trains of AFW) since this incident had (mostly) complete system failures. Other scenarios that see partial system failures (e.g., one pump fails out of three redundant pumps) are more complicated, with respect to the PSA mapping, and would have to be handled appropriately (Smith, 1998).

An additional complication from the PSA analysis was the modeling of partial failure of the MFW system for the first one-half minute of the incident. Initially, MFW pump 1 was failed while pump 2 continued to operate. The Surry PSA model does not have basic events for either pump 1 or pump 2 of MFW. Instead, the model has a single event representing failure of the MFW system, meaning it is either completely failed or completely working. Thus, this issue is one of applicability of the PSA model for the task of incident investigation. While we did not spend time specifically evaluating the PSA model itself for its overall applicability to the framework of incident management, we did run into PSA issues that would need to be resolved.

To model partial failure of the MFW system, we could use the information on the overall system failure probability to deduce a partial-failure probability. From the Surry NUREG-1150 document, we found that:

$$P(\text{MFW}) \quad = \quad 2.9\text{E-}3 \; .$$

This failure probability is assumed to be produced by an equal contribution from each of the two trains of MFW, or

$$\begin{aligned} 2.9\text{E-}3 \quad &= \quad \text{Pump Train 1} \times \text{Pump Train 2} \; . \\ &= \quad (\text{Pump Train})^2 \end{aligned}$$

Table 1. PSA configuration parameters for the Davis-Besse incident.

Configuration	Time (min.)	Adjusted PSA components	Notes
1	0^-	none	Baseline calculation
2	0^+	**M** = 5.39E-2	From the Surry NUREG-1150 document, P(MFW) = 2.9E-3. This probability is assumed to be produced by an equal probability from each of two trains of MFW, or 2.9E-3 = Pump Train 1 × Pump Train 2 . = (Pump Train)^2 Thus, P(MFW $\mid$ Pump Train 1 failed) = 5.39E-2.
3	0.5	**M** = 5.39E-2 **IE-T** = 1.0 All other initiating events = 0.0	Reactor trip. Assume that "coast down" of MFW pump 2 is sufficient to provide feedwater flow.
4	5.0	**M** = 1, **IE-T2** = 1.0 All other initiating events = 0.0	Complete loss of MFW with reactor trip.
5	6.0	**M** = 1, **IE-T2** = 1.0 All other initiating events = 0.0 The following events set to a probability of 1.0 **AFW-CCF-FS-FW3AB** **AFW-MDP-FR-3A1HR** **AFW-MDP-FR-3A24H** **AFW-MDP-FR-3A6HR** **AFW-MDP-FR-3B1HR** **AFW-MDP-FR-3B24H** **AFW-MDP-FR-3B6HR** **AFW-MDP-FS** **AFW-MDP-FS-FW3A** **AFW-MDP-FS-FW3B** **AFW-TDP-FR-2P1HR** **AFW-TDP-FR-2P24H** **AFW-TDP-FR-2P6HR** **AFW-TDP-FS-FW2**	Complete loss of MFW with reactor trip. Isolation of AFW.
6	9.0	Same as configuration 5	AFW system is still inoperable.

Configuration	Time (min.)	Adjusted PSA components	Notes
7	16.5	Same as configuration 5	Surry does not have a “start-up” feedwater pump.
8	19.0	Same as configuration 4	

Notes:

IE-T2	LOSS OF MAIN FEEDWATER
IE-T	FULL PWR TRANSIENT EV REQ RX SCRAM
M	FAILURE OF MAIN FEEDWATER
AFW-CCF-FS-FW3AB	COMMON CAUSE FAILURE OF AFW MOTOR DRIVEN PUMP
AFW-MDP-FR-3A1HR	MDP AFW 3A FAILS TO RUN 1 HOUR
AFW-MDP-FR-3A24H	AFW MOTOR DRIVEN PUMP 3A FAILS TO RUN 24 HRS
AFW-MDP-FR-3A6HR	MDP AFW 3A FAILS TO RUN 6 HOURS
AFW-MDP-FR-3B1HR	MDP AFW 3B FAILS TO RUN 1 HOUR
AFW-MDP-FR-3B24H	AFW MOTOR DRIVEN PUMP 3B FAILS TO RUN 24 HRS
AFW-MDP-FR-3B6HR	MDP AFW 3B FAILS TO RUN 6 HOURS
AFW-MDP-FS	AFW MDP FAILS TO START
AFW-MDP-FS-FW3A	MDP AFW 3A FAILS TO START
AFW-MDP-FS-FW3B	MDP AFW 3B FAILS TO START
AFW-TDP-FR-2P1HR	AFW TURBINE DRIVEN PUMP 2 FAILS TO RUN 1 HOUR
AFW-TDP-FR-2P24H	AFW TURBINE DRIVEN PUMP 2 FAILS TO RUN 24 HRS
AFW-TDP-FR-2P6HR	AFW TURBINE DRIVEN PUMP 2 FAILS TO RUN FOR 6 HOURS
AFW-TDP-FS-FW2	TURBINE DRIVEN AFW PUMP FAILS TO START

Consequently, for the configuration where only one MFW pump is inoperable, we used

P(MFW | Pump Train 1 failed) = 5.39E-2.

This value (5.39E-2) would then need to be put into the Surry PSA for the **M** basic event (note that this calculation is conservative since we are splitting the entire unavailability into only two parts) . This modification was accomplished by using the SAPHIRE “change set” feature. Change sets allows an analyst to set up multiple scenarios directly within the PSA model itself so that analysis (e.g., generating cut sets, evaluating importance measures, determining uncertainty contributions) for a particular configuration can be run without having to alter the base PSA model. Then, for this configuration (i.e., configuration 2), the PSA model is resolved by regenerating the overall core damage minimal cut sets using the new basic event data. As can be seen in Table 1, other configurations have additional basic event modification that need to be accounted for, thereby representing the incident complication as a function of time during the scenario. We will see later that this process of discritization of the incident into configurations allows us to evaluate decision alternatives (in time) via a formal decision-making process (e.g., influence diagrams or decision trees). Of course, within the form decision-making tools, we must account for timing considerations (e.g., time to restore a component, time to core melt) in order to prioritize decisions.

Now that we have determined the configurations during the incident and have decomposed the PSA basic events into two groups, those to be modified for a configuration and those left untouched. the next step is to perform the PSA analysis. To generate the minimal cut sets for core damage, we select the SAPHIRE change set for a particular configuration, initialize the PSA data, and then generate minimal cut sets for all accident sequences modeled in the PSA. Note that for configurations 3 through 8, we specifically model the fact that we saw a transient initiating event (basic event **IE-T** in the PSA model) by setting the probability of a transient event to a value of one and the remaining initiating event to a probability of zero. It is possible that we could experience two initiating events simultaneously (say a loss of coolant accident independent of the transient), but the probability of such a situation is small and, consequently, ignoring the other initiating events does not impact the overall numerical results.

Since, for configurations 3 through 8, we model only one initiating event (the transient), we could just ignore the non-transient sequences (they should have zero probability). But, telling the SAPHIRE software to evaluate these additional sequences (even though they end up with zero probability) results in a negligible increase in the analysis time (a couple of seconds). The overall analysis time for a configuration is on the order of 50 to 60 seconds for the Surry PSA model at a sequence truncation level of 1E-10 (i.e., discard any minimal cut set with probability *below* a value of 1E-10).

An additional note to the PSA analysis process is that we do not need to resolve the PSA for every configuration. As noted in Table 1, three of the configurations (6, 7, and 8) are the same as earlier configurations (5, 5, and 4, respectively). Thus, we need to resolve the PSA model only five times (i.e., configurations 1 through 5) in order to effectively represent the entire “risk profile” for the incident from start to finish.

First, let us evaluate the PSA results for configuration 1. Remember that configuration 1 has been defined as the state where the plant is in a normal (or nominal) configuration. The PSA result for this configuration are summarized in Table 2. A variety of information is contained within this table; each section of the table deserves a discussion in turn.

The first result shown in the table is the overall core damage frequency (CDF) conditional upon being in configuration 1 (which just happens to be the nominal configuration). The value of this CDF is 8.6E-5 per reactor year. In other papers, it has been discussed why the CDF is not a very good metric for tracking risk over a period of time (Smith, 1998). One of the reasons for the reluctance to use CDF is that it is difficult to compare two configurations solely based upon CDF. Instead, a core damage probability (CDP) is generally preferred to the CDF for time-based risk scenarios like those evaluated in the paper and envisioned for an incident management system. Note that one could turn a CDF into a CDP, or conditional CDP (CCDP), by knowing the duration applicable to the CDF. For example, if the plant were to be operated in its nominal state for 100 hours, the probability of seeing one or more core damage events over this duration is given as

$$\begin{aligned} P(CD \mid 100 \ hours, \ nominal \ conditions) &= 1 - e^{-\lambda_{CD} t} \\ &= 1 - e^{-8.6\times10^{-5}/yr\,(100\,hr)(1\,yr/8760\,hr)} = 9.8\times10^{-7} \quad . \end{aligned}$$

where λ_{CD} = the core damage frequency
t = the time duration.

This evaluation of the CCDP over the 100 hour duration assumes that the core damage scenarios of interest satisfy all of the assumptions of Poisson events. But, for the analysis in this paper, we effectively ignore the configuration where the plant is in its nominal state since, from a decision-framework point of view, it is not very interesting.

The second result shown in Table 2 is the sequence risk results. We have effectively ranked all of the accident sequences by highest frequency to lowest frequence. In the table, we show just the top 10 sequences. Notice that, during nominal situations, a transient with MFW available is the most likely event to occur that leads to core damage. Further, core damage sequences where the plant lost MFW are fourth most frequent. Consequently, it should not be surprising that the Davis-Besse loss of feedwater event did actually happen and came relatively close to damaging the reactor core.

The third results shown in Table 2 are for the importance measures from the accident sequences. We first display the Fussell-Vesely measures and then the Risk Achievement Worth (RAW) measures.

Table 2. Results of the PSA (Davis-Besse) conditional upon configuration 1 (truncation of 1E-10).

Metric	Results for Configuration 1		
	Summary Risk Results		
CDF	8.6E-5/yr		
	Sequence Risk Results		
Sequences with the largest absolute frequency	FT3	15-08	TURBINE TRIP WITH MFW
	FT1S	08	SBO-SLOCA DOMINANT SEQUENCE RCP SEAL LOCA
	FT1S	04	SBO-BATT DOMINANT SEQUENCE SBO BATT DEPLETION
	FT2	14-08	LOSS OF MFW
	FT1SB	06	SBO-SLOCA2 DOMINANT SEQUENCE RCP SEAL LOCA
	FT1S	20	SBO-L DOMINANT SEQUENCE AFW FAILURE
	FT1S	19	SBO-SLOCA DOMINANT SEQUENCE RCP SEAL LOCA
	FS3	23	S3D1 DOMINANT SEQUENCE VERY SMALL LOCA INJ FAILURE
	FT1S	15	SBO-BATT DOMINANT SEQUENCE SBO BATT DEPLETION
	FT3	14-20	TURBINE TRIP WITH MFW
	Basic Event Results		
Basic events with the largest Fussell-Vesely importance measure	R	4.636E-001	FAILURE TO MANUALLY SCRAM THE REACTOR
	K	4.624E-001	FAILURE OF RPS TO SCRAM THE REACTOR
	T	4.370E-001	TURBINE TRIP SUBSEQUENT TO ATWS
	IE-T3	4.316E-001	TURBINE TRIP WITH MAIN FEEDWATER AVAILABLE
	IE-T1S	3.047E-001	LOSS OF OFFSITE POWER
	REC-XHE-FO-DGHWS	1.402E-001	OP FAILS TO REC A DG FM HW FAIL IN 3 HR
	RCP-LOCA-750-90M	1.251E-001	750 GPM RCP SEAL LOCA AT 90 MIN
	OEP-DGN-FS-DG01	1.222E-001	DIESEL GENERATOR #1 FAILS TO START
	NRAC-216MIN	1.207E-001	NON-RECOVERY AC PWR W/IN 216 MIN OF LOSP
	QS-SBO	1.025E-001	POWER CONVERSION SYS: STM GENERATOR INTEGRITY
Basic events with the largest Risk Achievement Worth importance measure	V-TRAIN-1	1.158E+004	INTERFACING LOCA FM RCS LOOP 1 TO LPI
	V-TRAIN-2	1.158E+004	INTERFACING LOCA FM RCS LOOP 2 TO LPI
	V-TRAIN-3	1.158E+004	INTERFACING LOCA FM RCS LOOP 3 TO LPI
	K	6.953E+003	FAILURE OF RPS TO SCRAM THE REACTOR
	RWT-TNK-LF-RWST	2.776E+002	INSUFFICIENT WATER AVAILABLE FROM THE RWST
	HPI-CCF-FT-115BD	4.171E+001	COMMON CAUSE FAILURE OF MOVS 1115B AND 1115D
	RMT-CCF-FA-MSCAL	3.698E+001	COMMON CAUSE FAILURE RMT DUE TO MISCALIBRATION
	T7K	2.066E+001	FAILURE OF RPS TO SCRAM THE RX
	ACC-MOV-PG-1865B	1.835E+001	ACC MOTOR OPERATED VALVE 1865B PLUGGED
	ACC-MOV-PG-1865C	1.835E+001	ACC MOTOR OPERATED VALVE 1865C PLUGGED

The Fussell-Vesely measure is the ratio of the sum of the frequencies of all accident sequences containing a basic event of interest over the nominal CDF. The RAW is the ratio of the CDF that results by assuming that the basic event is unavailable over the nominal CDF. These two measures attempt to reveal two different types of information, but they are crude metrics of risk. For example, Cheok, Parry, and Sherry (1998) argue that Fussell-Vesely and RAW are "gross measures of the importance of a basic event," because they measure changes in risk only in extreme cases (i.e., the basic event is either perfect or completely unavailable). An important observation is that "the importance measures are, for the most part, not directly related to the risk changes associated with the change being evaluated" (Cheok, Parry, and Sherry, 1998). Fleming (1996) also lists a number of limitations and observes that "…RAW is not defined for initiating events…" Further, he notes that "To develop meaningful conclusions from a PSA, it is necessary to take into account a deep understanding of the principal contributors to risk." The latter are not normally part of the insights gained from importance measures.

A recent report from the Advisory Committee on Reactor Safeguards (ACRS, 1999) lists several issues related to the use of importance measures. It is pointed out that the importance measures of a particular basic event are sensitive functions of the conservative assumptions that may be made in parts of the PRA that do not involve that basic event. Thus, a conservative fire risk assessment may distort the risk significance of an event that has nothing to do with fires. Furthermore, the calculation of RAW requires the assumption that the basic event is unavailable. This calculation may be much more involved than simply setting the unavailability of the basic event equal to unity. The assumption of a basic event being unavailable may affect several terms in the PRA. For example, the event may also appear in the probability of a common-cause failure and in the probability of recovery actions being successful (Smith, 1998). Other problems with importance measures are discussed by Vesely (1998), one of the developers of the FV measure. Because of the central role that importance measures play in many risk-informed applications and could play in a formal incident management advisory system, it is evident that improvements are needed in this area.

Tables 3, 4, and 5 show the PSA analysis results for the next three configurations (2, 3, and 4, respectively). We show similar results to those shown in Table 2 (note though that we also list the top eight minimal cut sets for configuration 4). Looking at the CCDPs for these three configurations, it should be evident that the risk (as measured by the CCDP) is increasing as the incident progresses in time. This increasing risk is due to the fact that, as time progresses, additional component failures or other complications are resulting in changes to the plant state. We will also demonstrate that as the incident progresses through time, the results of risk metrics such as the importance measures vary through time. This implies that decisions of which action(s) to take over the course of an incident also vary as a function of time. We will also demonstrate that the PSA (and resultant calculations) are useful for developing decision strategies during the incident time frame.

Table 3. Results of the PSA (Davis-Besse) conditional upon configuration 2 (truncation of 1E-10).

Metric	Results for Configuration 2		
	Summary Risk Results		
CCDF	8.7E-5/yr (CCDP over 0.5 minute duration = 1.7E-10)		
	Sequence Risk Results		
Sequences with the largest absolute frequency	FT3	15-08	TURBINE TRIP WITH MFW
	FT1S	08	SBO-SLOCA DOMINANT SEQUENCE RCP SEAL LOCA
	FT1S	04	SBO-BATT DOMINANT SEQUENCE SBO BATT DEPLETION
	FT2	14-08	LOSS OF MFW
	FT1SB	06	SBO-SLOCA2 DOMINANT SEQUENCE RCP SEAL LOCA
	FT1S	20	SBO-L DOMINANT SEQUENCE AFW FAILURE
	FT1S	19	SBO-SLOCA DOMINANT SEQUENCE RCP SEAL LOCA
	FS3	23	S3D1 DOMINANT SEQUENCE VERY SMALL LOCA INJ FAILURE
	FT1S	15	SBO-BATT DOMINANT SEQUENCE SBO BATT DEPLETION
	FT3	14-20	TURBINE TRIP WITH MFW
	Basic Event Results		
Basic events with the largest Fussell-Vesely importance measure	R	4.601E-001	FAILURE TO MANUALLY SCRAM THE REACTOR
	K	4.589E-001	FAILURE OF RPS TO SCRAM THE REACTOR
	IE-T3	4.358E-001	TURBINE TRIP WITH MAIN FEEDWATER AVAILABLE
	T	4.337E-001	TURBINE TRIP SUBSEQUENT TO ATWS
	IE-T1S	3.024E-001	LOSS OF OFFSITE POWER
	REC-XHE-FO-DGHWS	1.392E-001	OP FAILS TO REC A DG FM HW FAIL IN 3 HR
	RCP-LOCA-750-90M	1.241E-001	750 GPM RCP SEAL LOCA AT 90 MIN
	OEP-DGN-FS-DG01	1.213E-001	DIESEL GENERATOR #1 FAILS TO START
	NRAC-216MIN	1.198E-001	NON-RECOVERY AC PWR W/IN 216 MIN OF LOSP
	QS-SBO	1.017E-001	POWER CONVERSION SYSTEM: STM GENERATOR INTEGRITY
Basic events with the largest Risk Achievement Worth importance measure	V-TRAIN-1	1.149E+004	INTERFACING LOCA FM RCS LOOP 1 TO LPI
	V-TRAIN-2	1.149E+004	INTERFACING LOCA FM RCS LOOP 2 TO LPI
	V-TRAIN-3	1.149E+004	INTERFACING LOCA FM RCS LOOP 3 TO LPI
	K	6.901E+003	FAILURE OF RPS TO SCRAM THE REACTOR
	RWT-TNK-LF-RWST	2.755E+002	INSUFFICIENT WATER AVAILABLE FROM THE RWST
	HPI-CCF-FT-115BD	4.145E+001	COMMON CAUSE FAILURE OF MOVS 1115B AND 1115D
	RMT-CCF-FA-MSCAL	3.676E+001	COMMON CAUSE FAILURE RMT DUE TO MISCALIBRATION
	T7K	2.051E+001	FAILURE OF RPS TO SCRAM THE RX
	ACC-MOV-PG-1865B	1.822E+001	ACC MOTOR OPERATED VALVE 1865B PLUGGED
	ACC-MOV-PG-1865C	1.822E+001	ACC MOTOR OPERATED VALVE 1865C PLUGGED

Table 4. Results of the PSA (Davis-Besse) conditional upon configuration 3 (truncation of 1E-10).

Metric	Results for Configuration 3 (accident time = 0.5 min)		
Summary Risk Results			
CCDP	1.1E-7		
Sequence Risk Results			
Sequences with the largest absolute frequency	FTKT	10	ATWS - FULL POWER TRANSIENT
	FTKT	12	ATWS - FULL POWER TRANSIENT
	FTKT	09	ATWS - FULL POWER TRANSIENT
	FTKT	17	ATWS - FULL POWER TRANSIENT
	FTKT	15	ATWS - FULL POWER TRANSIENT
	FTKT	20	ATWS - FULL POWER TRANSIENT
	FT5A	13-14	LOSS OF DC BUS A
	FT5A	13-10	LOSS OF DC BUS A
	FT5A	13-11	LOSS OF DC BUS A
	FT5A	13-13	LOSS OF DC BUS A
Basic Event Results			
Basic events with the largest Fussell-Vesely importance measure	R	1.000E+000	FAILURE TO MANUALLY SCRAM THE REACTOR
	K	1.000E+000	FAILURE OF RPS TO SCRAM THE REACTOR
	Z	5.973E-001	MTC UNFAVORABLE
	HPI-MOV-FT-1350	1.569E-001	HPI MOV 1350 FAILS TO OPEN
	PCS-XHE-FO-TBTRP	1.139E-001	OP FAILS TO TRIP MAIN TURBINE
	PPS-XHE-FO-EMBOR	5.229E-002	OPER FAILS TO CORRECTLY PERFORM EMERG BORATION
	PPS-MOV-FC-1536	2.400E-002	BLOCK VALVE MOV 1536 SHUT DUE TO LEAKING PORV
	PPS-MOV-FC-1535	2.400E-002	BLOCK VALVE MOV 1535 SHUT DUE TO LEAKING PORV
	PPS-CCF-FT-15356	1.647E-002	COMMON CAUSE FAILURE OF PORV BLOCKING VALVES
	AFW-PSF-FC-XCONN	7.843E-003	FLOW DIVERSION TO UNIT 2 THRU XCONNECT
Basic events with the largest Risk Achievement Worth importance measure	K	1.666E+004	FAILURE OF RPS TO SCRAM THE REACTOR
	AFW-CCF-LK-STMBD	5.328E+001	UNDETECT LEAKAGE THRU CV27 CV58 CV89
	AFW-PSF-FC-XCONN	5.328E+001	FLOW DIVERSION TO UNIT 2 THRU XCONNECT
	PPS-XHE-FO-EMBOR	5.323E+001	OPER FAILS TO CORRECTLY PERFORM EMERG BORATION
	HPI-MOV-FT-1350	5.313E+001	HPI MOV 1350 FAILS TO OPEN
	ACP-CRB-CO-14H15	4.378E+001	AC CIRCUIT BREAKER 14H15 TRANSFERS OPEN
	ACP-CRB-CO-14H13	4.378E+001	AC CIRCUIT BREAKER 14H13 TRANSFERS OPEN
	ACP-CRB-CO-15H7	4.378E+001	AC CIRCUIT BREAKER 15H7 TRANSFERS OPEN
	CVC-MDP-FR-2A1HR	4.378E+001	BORIC ACID TRANSFER PUMP FAIL TO RUN 1 HOUR
	HPI-MOV-PG-1350	4.378E+001	HPI MOTOR OPERATED VALVE 1350 PLUGGED

Table 5. Results of the PSA (Davis-Besse) conditional upon configuration 4 (truncation of 1E-10).

Metric	Results for Configuration 4 (accident time = 5 min)		
	Summary Risk Results		
CCDP	6.9E-6		
	Sequence Risk Results		
Sequences with the largest absolute frequency	FT2	14-08	LOSS OF MFW
	FT2	11	T2LP DOMINANT SEQUENCE LMFW/AFWW F&B FAILS
	FT2	12	T2LD2 DOMINANT SEQUENCE LMFW/AFWW F&B FAILS
	FT2	13-20	LOSS OF MFW
	FT2	03	LOSS OF MFW
	FT2	13-02	LOSS OF MFW
	FT2	14-09	LOSS OF MFW
	FT2	14-11	LOSS OF MFW
	FT2	06	LOSS OF MFW
	FT2	14-16	LOSS OF MFW
	Basic Event Results		
Basic events with the largest Fussell-Vesely importance measure	R	6.737E-001	FAILURE TO MANUALLY SCRAM THE REACTOR
	K	6.736E-001	FAILURE OF RPS TO SCRAM THE REACTOR
	T	6.598E-001	TURBINE TRIP SUBSEQUENT TO ATWS
	AFW-XHE-FO-UNIT2	2.570E-001	OP FAILS TO XCONN AFW TRANSIENTS
	HPI-XHE-FO-FDBLD	1.239E-001	OP FAILS TO ESTABLISH FEED AND BLEED OPERATIO
	AFW-PSF-FC-XCONN	1.154E-001	FLOW DIVERSION TO UNIT 2 THRU XCONNECT
	AFW-CCF-LK-STMBD	7.694E-002	UNDETECT LEAKAGE THRU CV27 CV58 CV89
	PPS-XHE-FO-PORVS	7.673E-002	FAILURE OF THE OP TO OPEN BOTH PORVS (F&B)
	PORV-DEMAND-T	5.130E-002	PROB RCS PORV IS DEMANDED PROB RCS PORV IS DEMANDED
	AFW-TDP-FR-2P24H	3.901E-002	AFW TURBINE DRIVEN PUMP 2 FAILS TO RUN 24 HRS
Basic events with the largest Risk Achievement Worth importance measure	AFW-PSF-FC-XCONN	7.690E+002	FLOW DIVERSION TO UNIT 2 THRU XCONNECT
	AFW-CCF-LK-STMBD	7.690E+002	UNDETECT LEAKAGE THRU CV27 CV58 CV89
	HPI-CKV-FT-CV225	8.210E+001	CHECK VALVE CV225 FAILS TO OPEN
	RWT-TNK-LF-RWST	8.114E+001	INSUFFICIENT WATER AVAILABLE FROM THE RWST
	HPI-CCF-FT-867CD	5.124E+001	COMMON CAUSE FAILURE OF HPI MOVS 1867C 1867D
	HPI-CCF-FT-115BD	2.738E+001	COMMON CAUSE FAILURE OF MOVS 1115B AND 1115D
	HPI-CKV-FT-CV25	2.732E+001	CHECK VALVE CV25 FAILS TO OPEN
	HPI-CKV-FT-CV410	2.732E+001	CHECK VALVE CV410 FAILS TO OPEN
	AFW-XHE-FO-UNIT2	7.883E+000	OP FAILS TO XCONN AFW TRANSIENTS

Metric

Results for Configuration 4 (accident time = 5 min)

Cut Set Results

```
 Cut    CutSet   Prob/
 No.      %      Freq.      Basic Event                Description
------  -----  ---------  -------------------------  -----------------------------------------------------------
     1    0.0   4.5E-006  IE-T2                      LOSS OF MAIN FEEDWATER
                          K                          FAILURE OF RPS TO SCRAM THE REACTOR
                          /PL                        PROBABILITY OF INITIAL POWER LEVEL BELOW 25
                          R                          FAILURE TO MANUALLY SCRAM THE REACTOR
                          T                          TURBINE TRIP SUBSEQUENT TO ATWS
                          /Z                         MTC UNFAVORABLE
                          /Z1                        MTC LOW
     2    0.0   3.8E-007  IE-T2                      LOSS OF MAIN FEEDWATER
                          AFW-PSF-FC-XCONN           FLOW DIVERSION TO UNIT 2 THRU XCONNECT
                          AFW-XHE-FO-UNIT2           OP FAILS TO XCONN AFW  TRANSIENTS
                          HPI-XHE-FO-FDBLD           OP FAILS TO ESTABLISH FEED AND BLEED OPERATIO
                          /K                         FAILURE OF RPS TO SCRAM THE REACTOR
     3    0.0   2.6E-007  IE-T2                      LOSS OF MAIN FEEDWATER
                          AFW-CCF-LK-STMBD           UNDETECT LEAKAGE THRU CV27  CV58  CV89
                          AFW-XHE-FO-UNIT2           OP FAILS TO XCONN AFW  TRANSIENTS
                          HPI-XHE-FO-FDBLD           OP FAILS TO ESTABLISH FEED AND BLEED OPERATIO
                          /K                         FAILURE OF RPS TO SCRAM THE REACTOR
     4    0.0   2.4E-007  IE-T2                      LOSS OF MAIN FEEDWATER
                          AFW-PSF-FC-XCONN           FLOW DIVERSION TO UNIT 2 THRU XCONNECT
                          AFW-XHE-FO-UNIT2           OP FAILS TO XCONN AFW  TRANSIENTS
                          /K                         FAILURE OF RPS TO SCRAM THE REACTOR
                          PPS-XHE-FO-PORVS           FAILURE OF THE OP TO OPEN BOTH PORVS (F&B)
     5    0.0   1.6E-007  IE-T2                      LOSS OF MAIN FEEDWATER
                          AFW-CCF-LK-STMBD           UNDETECT LEAKAGE THRU CV27  CV58  CV89
                          AFW-XHE-FO-UNIT2           OP FAILS TO XCONN AFW  TRANSIENTS
                          /K                         FAILURE OF RPS TO SCRAM THE REACTOR
                          PPS-XHE-FO-PORVS           FAILURE OF THE OP TO OPEN BOTH PORVS (F&B)
     6    0.0   1.0E-007  IE-T2                      LOSS OF MAIN FEEDWATER
                          AFW-CCF-FS-FW3AB           COMMON CAUSE FAILURE OF AFW MOTOR DRIVEN PUMP
                          AFW-TDP-FR-2P24H           AFW TURBINE DRIVEN PUMP 2 FAILS TO RUN 24 HRS
                          AFW-XHE-FO-UNIT2           OP FAILS TO XCONN AFW  TRANSIENTS
                          HPI-XHE-FO-FDBLD           OP FAILS TO ESTABLISH FEED AND BLEED OPERATIO
                          /K                         FAILURE OF RPS TO SCRAM THE REACTOR
     7    0.0   6.5E-008  IE-T2                      LOSS OF MAIN FEEDWATER
                          AFW-PSF-FC-XCONN           FLOW DIVERSION TO UNIT 2 THRU XCONNECT
                          AFW-XHE-FO-UNIT2           OP FAILS TO XCONN AFW  TRANSIENTS
                          /K                         FAILURE OF RPS TO SCRAM THE REACTOR
                          PPS-MOV-FC-1535            BLOCK VALVE MOV 1535 SHUT DUE TO LEAKING PORV
                          PPS-MOV-FT-1535            PORV BLOCK VALVE 1535 FAILS TO OPEN
     8    0.0   6.5E-008  IE-T2                      LOSS OF MAIN FEEDWATER
                          AFW-PSF-FC-XCONN           FLOW DIVERSION TO UNIT 2 THRU XCONNECT
                          AFW-XHE-FO-UNIT2           OP FAILS TO XCONN AFW  TRANSIENTS
                          /K                         FAILURE OF RPS TO SCRAM THE REACTOR
                          PPS-MOV-FC-1536            BLOCK VALVE MOV 1536 SHUT DUE TO LEAKING PORV
                          PPS-MOV-FT-1536            PORV BLOCK VALVE 1536 FAILS TO OPEN
```

Lastly, we come to the configuration 5. This configuration represents the closest to core damage that we get throughout the entire incident. The results of the PSA calculation are shown in Table 6. As can be seen in the table, the calculated CCDP is about 1E-2, which is a very high CCDP. This CCDP implies that if this scenario were experienced 100 times, we would expect to see one of the scenarios to end in significant core damage. CCDPs of this magnitude typically draw a high-level of attention from regulators such as the U.S. Nuclear Regulatory Commission (in fact, following the Davis-Besse event, an entire team of NRC regulators visited the plant to inspect what caused the event, what lessons can be learned, and were improvements made to the facility (NRC, 1985).

Configurations 5, 6, and 7 represents the plant state from time 6 min to 16.5 min during the incident. Looking at the PSA results (namely, the importance measures and the dominate minimal cut sets), it is evident that two items are important during these configurations: (1) operability of AFW and (2) utilization of "feed-and-bleed" cooling. Consequently, from the PSA, we could extract applicable decisions that could remedy the situation, decisions that we believe should be evaluated in a formal decision-making framework. And, in Section 4, we will revisit these potential decision via use of influence diagrams and decision trees. But, for now, it is enough to realize that the PSA is a vital tool (in conjunction with standard constraints such as the operating procedures and technical specifications) in the determination of decision during the course of an incident.

While having decision alternatives is important, equally important to the decision process is the timing of the scenario to this point and relative times for decision alternatives. For example, if the situation is such that core damage is imminent (say within five minutes) but it will take a long time to restore AFW (say one hour), an incident management system based upon formal decision-making tools would suggest an immediate move to feed-and-bleed cooling. Since we are dealing with times that have both aleatory and epistemic uncertainties associated with them, a handle on the uncertainty from the PSA model, thermohydraulics, and response times will be a necessity for any realistic incident management system. For the trial investigations discussed in this report, we only evaluated the uncertainties in a cursory fashion, and then only in the formal decision-making portion of the analysis.

At this point in the incident, we have seen how the scenario becomes more complicated over time. This complication is further illustrated by pointing out, on the PSA event tree diagram, how the plant (and operators at the plant) proceeded from left to right across the loss of MFW event tree. This illustration is shown in Figure 1. The incident started out as a partial loss of MFW and then turned into a complete loss of MFW with the closure of the MSIVs. At that point, the plant was experiencing a loss of MFW initiating event and were at the starting node of the event tree shown in Figure 1. As the incident continued, the RO1 attempted to start the AFW system (at time 6 min), but in fact isolated AFW. Consequently, at time 6 min in Figure 1, we follow the down branch under the AFW event tree top event (node "L") representing failure of the AFW.

Table 6. Results of the PSA (Davis-Besse) conditional upon configuration 5 (truncation of 1E-10).

Metric	Results for Configuration 5 (accident time = +6 min)		
	Summary Risk Results		
CCDP	1.1E-2		
	Sequence Risk Results		
Sequences with the largest absolute frequency	FT2	11	T2LP DOMINANT SEQUENCE LMFW/AFWW F&B FAILS
	FT2	12	T2LD2 DOMINANT SEQUENCE LMFW/AFWW F&B FAILS
	FT2	06	LOSS OF MFW
	FT2	14-14	LOSS OF MFW
	FT2	14-08	LOSS OF MFW
	FT2	09	LOSS OF MFW
	FT2	14-19	LOSS OF MFW
	FT2	13-19	LOSS OF MFW
	FT2	10	LOSS OF MFW
	FT2	13-20	LOSS OF MFW
	Basic Event Results		
Basic events with the largest Fussell-Vesely importance measure	AFW-XHE-FO-UNIT2	9.981E-001	OP FAILS TO XCONN AFW TRANSIENTS
	AFW-TDP-FS-FW2	8.887E-001	TURBINE DRIVEN AFW PUMP FAILS TO START
	AFW-MDP-FS-FW3A	4.974E-001	MDP AFW 3A FAILS TO START
	AFW-MDP-FS-FW3B	4.973E-001	MDP AFW 3B FAILS TO START
	AFW-CCF-FS-FW3AB	4.958E-001	COMMON CAUSE FAILURE OF AFW MOTOR DRIVEN PUMP
	HPI-XHE-FO-FDBLD	4.823E-001	OP FAILS TO ESTABLISH FEED AND BLEED OPERATIO
	PPS-XHE-FO-PORVS	2.984E-001	FAILURE OF THE OP TO OPEN BOTH PORVS (F&B)
	AFW-TDP-FR-2P24H	9.970E-002	AFW TURBINE DRIVEN PUMP 2 FAILS TO RUN 24 HRS
	PPS-MOV-FC-1536	8.929E-002	BLOCK VALVE MOV 1536 SHUT DUE TO LEAKING PORV
	PPS-MOV-FC-1535	8.927E-002	BLOCK VALVE MOV 1535 SHUT DUE TO LEAKING PORV
Basic events with the largest Risk Achievement Worth importance measure	AFW-XHE-FO-UNIT2	2.419E+001	OP FAILS TO XCONN AFW TRANSIENTS
	RWT-TNK-LF-RWST	7.643E+000	INSUFFICIENT WATER AVAILABLE FROM THE RWST
	HPI-CCF-FT-867CD	7.626E+000	COMMON CAUSE FAILURE OF HPI MOVS 1867C 1867D
	LPR-CCF-FT-863AB	7.615E+000	COMMON CAUSE FAILURE OF MOV 1863A/B
	RMT-CCF-FA-MSCAL	7.615E+000	COMMON CAUSE FAILURE RMT DUE TO MISCALIBRATION
	HPI-CCF-FT-115BD	7.613E+000	COMMON CAUSE FAILURE OF MOVS 1115B AND 1115D
	HPI-CKV-FT-CV225	7.643E+000	CHECK VALVE CV225 FAILS TO OPEN
	HPI-CKV-FT-CV25	7.614E+000	CHECK VALVE CV25 FAILS TO OPEN
	HPI-CKV-FT-CV410	7.614E+000	CHECK VALVE CV410 FAILS TO OPEN
	DCP-BDC-ST-BUS1A	7.816E+000	125V DC BUS 1A BUSWORK FAILURE

Metric	Results for Configuration 5 (accident time = +6 min)

Cut Set Results

```
 Cut    CutSet   Prob/
 No.      %      Freq.     Basic Event                Description
------  -----  ---------  -------------------------  ----------------------------------------------------------
     1    0.0   2.6E-003  IE-T2                      LOSS OF MAIN FEEDWATER
                          AFW-CCF-FS-FW3AB           COMMON CAUSE FAILURE OF AFW MOTOR DRIVEN PUMP
                          AFW-TDP-FS-FW2             TURBINE DRIVEN AFW PUMP FAILS TO START
                          AFW-XHE-FO-UNIT2           OP FAILS TO XCONN AFW  TRANSIENTS
                          HPI-XHE-FO-FDBLD           OP FAILS TO ESTABLISH FEED AND BLEED OPERATION
                          /K                         FAILURE OF RPS TO SCRAM THE REACTOR
     2    0.0   2.6E-003  IE-T2                      LOSS OF MAIN FEEDWATER
                          AFW-MDP-FS-FW3A            MDP AFW 3A FAILS TO START
                          AFW-MDP-FS-FW3B            MDP AFW 3B FAILS TO START
                          AFW-TDP-FS-FW2             TURBINE DRIVEN AFW PUMP FAILS TO START
                          AFW-XHE-FO-UNIT2           OP FAILS TO XCONN AFW  TRANSIENTS
                          HPI-XHE-FO-FDBLD           OP FAILS TO ESTABLISH FEED AND BLEED OPERATION
                          /K                         FAILURE OF RPS TO SCRAM THE REACTOR
     3    0.0   1.6E-003  IE-T2                      LOSS OF MAIN FEEDWATER
                          AFW-CCF-FS-FW3AB           COMMON CAUSE FAILURE OF AFW MOTOR DRIVEN PUMP
                          AFW-TDP-FS-FW2             TURBINE DRIVEN AFW PUMP FAILS TO START
                          AFW-XHE-FO-UNIT2           OP FAILS TO XCONN AFW  TRANSIENTS
                          /K                         FAILURE OF RPS TO SCRAM THE REACTOR
                          PPS-XHE-FO-PORVS           FAILURE OF THE OP TO OPEN BOTH PORVS (F&B)
     4    0.0   1.6E-003  IE-T2                      LOSS OF MAIN FEEDWATER
                          AFW-MDP-FS-FW3A            MDP AFW 3A FAILS TO START
                          AFW-MDP-FS-FW3B            MDP AFW 3B FAILS TO START
                          AFW-TDP-FS-FW2             TURBINE DRIVEN AFW PUMP FAILS TO START
                          AFW-XHE-FO-UNIT2           OP FAILS TO XCONN AFW  TRANSIENTS
                          /K                         FAILURE OF RPS TO SCRAM THE REACTOR
                          PPS-XHE-FO-PORVS           FAILURE OF THE OP TO OPEN BOTH PORVS (F&B)
     5    0.0   4.3E-004  IE-T2                      LOSS OF MAIN FEEDWATER
                          AFW-CCF-FS-FW3AB           COMMON CAUSE FAILURE OF AFW MOTOR DRIVEN PUMP
                          AFW-TDP-FS-FW2             TURBINE DRIVEN AFW PUMP FAILS TO START
                          AFW-XHE-FO-UNIT2           OP FAILS TO XCONN AFW  TRANSIENTS
                          /K                         FAILURE OF RPS TO SCRAM THE REACTOR
                          PPS-MOV-FC-1535            BLOCK VALVE MOV 1535 SHUT DUE TO LEAKING PORV
                          PPS-MOV-FT-1535            PORV BLOCK VALVE 1535 FAILS TO OPEN
     6    0.0   4.3E-004  IE-T2                      LOSS OF MAIN FEEDWATER
                          AFW-CCF-FS-FW3AB           COMMON CAUSE FAILURE OF AFW MOTOR DRIVEN PUMP
                          AFW-TDP-FS-FW2             TURBINE DRIVEN AFW PUMP FAILS TO START
                          AFW-XHE-FO-UNIT2           OP FAILS TO XCONN AFW  TRANSIENTS
                          /K                         FAILURE OF RPS TO SCRAM THE REACTOR
                          PPS-MOV-FC-1536            BLOCK VALVE MOV 1536 SHUT DUE TO LEAKING PORV
                          PPS-MOV-FT-1536            PORV BLOCK VALVE 1536 FAILS TO OPEN
```

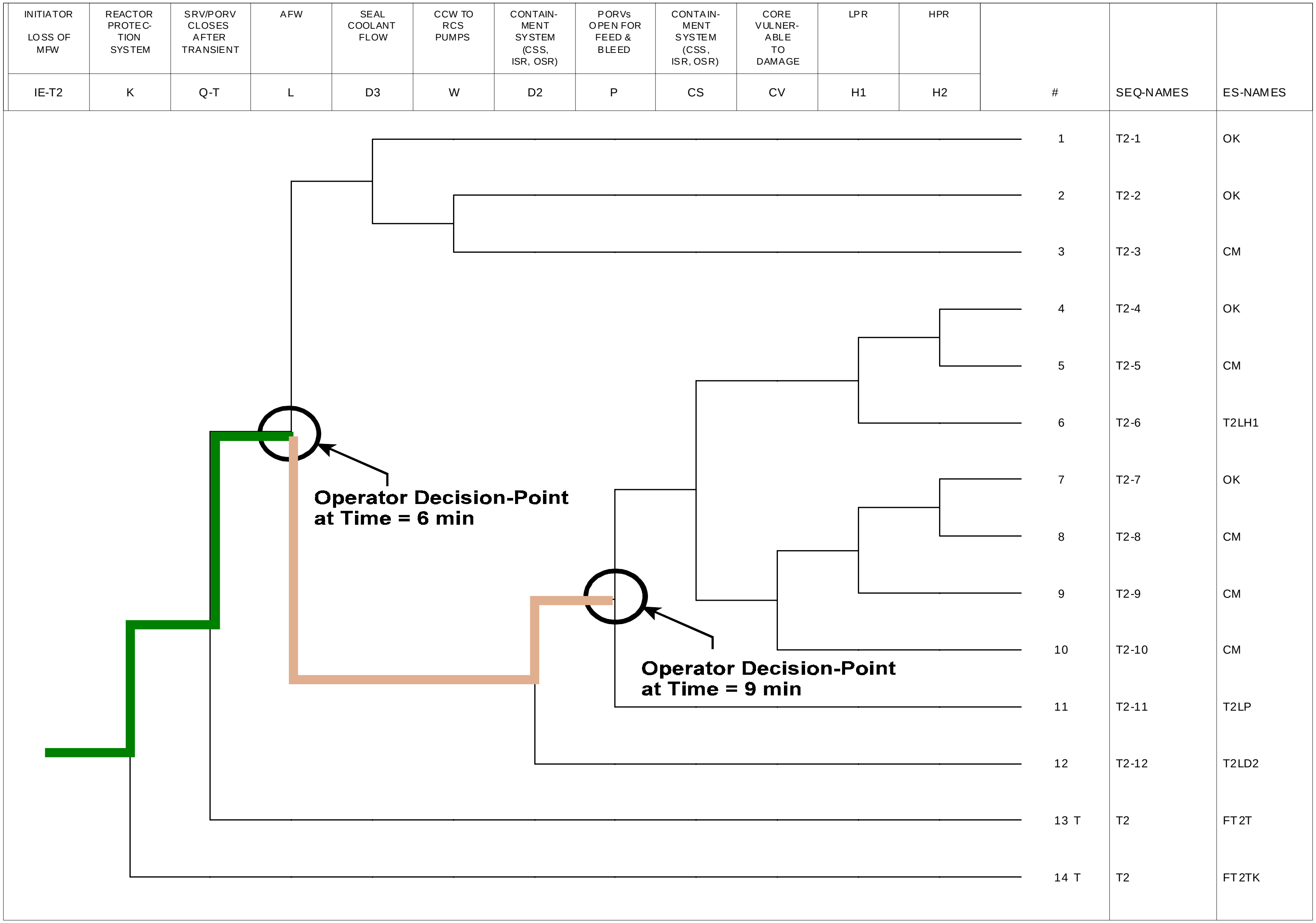

INITIATOR LOSS OF MFW
REACTOR PROTECTION SYSTEM
SRV/PORV CLOSES AFTER TRANSIENT
AFW
SEAL COOLANT FLOW
CCW TO RCS PUMPS
CONTAINMENT SYSTEM (CSS, ISR, OSR)
PORVs OPEN FOR FEED & BLEED
CONTAINMENT SYSTEM (CSS, ISR, OSR)
CORE VULNERABLE TO DAMAGE
LPR
HPR
IE-T2
K
Q-T
L
D3
W
D2
P
CS
CV
H1
H2
#
SEQ-NAMES
ES-NAMES
1 T2-1 OK
2 T2-2 OK
3 T2-3 CM
4 T2-4 OK
5 T2-5 CM
6 T2-6 T2LH1
7 T2-7 OK
8 T2-8 CM
9 T2-9 CM
10 T2-10 CM
11 T2-11 T2LP
12 T2-12 T2LD2
13 T T2 FT2T
14 T T2 FT2TK
Operator Decision-Point at Time = 6 min
Operator Decision-Point at Time = 9 min

Figure 1. PSA representation of Davis-Besse event through time showing the two critical decision nodes.

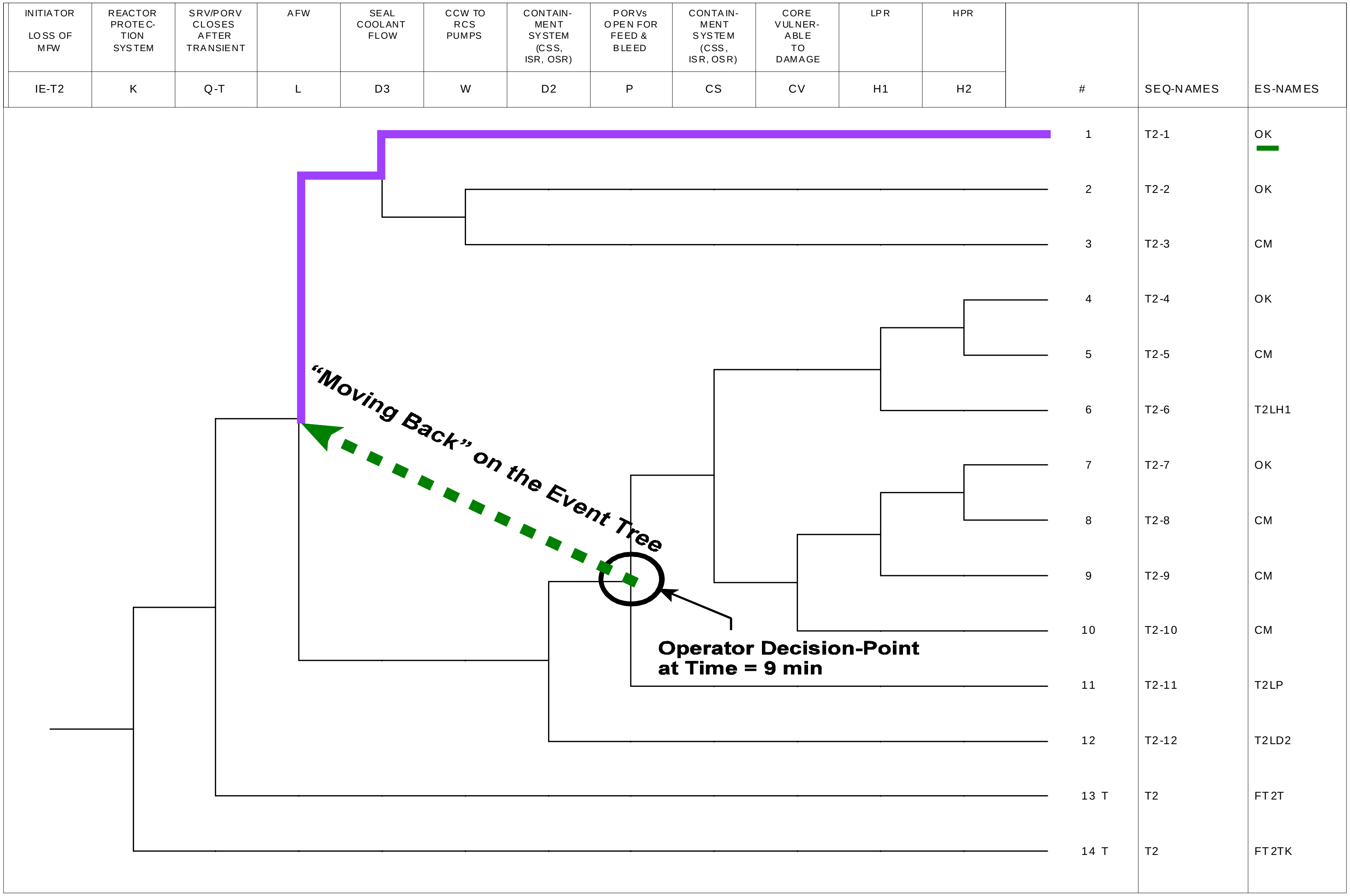
Continuing on in the sequence represented in Figure 1, at time 9 min, we have reached to point where SRO1 had to ultimately make the decision of to proceed to feed-and-bleed cooling or continue trying to restore the inoperable AFW pumps. At this point on the event tree, we do not proceed since feed-and-bleed cooling was not called for in the Davis-Besse event (thus, it did not either fail or succeed). Instead, by taking the decision to restore AFW, SRO1 was effectively attempting to "move back" on the event tree in PSA space. One would desire to "move back" on the event tree in order to end up on a sequence that does not result in core damage (an "OK" sequence). As illustrated in Figure 2, "moving back" for the Davis-Besse incident at a time of 9 min implies that the operators are attempting to restore functionality of the AFW system (i.e., an up branch under the "L" node of the event tree).

At this point in the scenario, the operators are faced with a serious situation. They have lost all feedwater, thereby causing the primary system to heat up (from the loss of the heat sink). It is unsure that AFW will be repairable and there is a reluctance to go to feed-and-bleed cooling. Rather than proceeding with the scenario, let us step back and review the critical decisions and see how the PSA could assist in the decision-making at these critical points in time.

At a time of almost 6 minutes, the critical decisions faced by the operating crew (and ultimately decided by SRO1) were:

Decision A | t = 6 min	Wait for AFW to actuate automatically
Decision B | t = 6 min	Manually actuate AFW via an instrument panel in the control room

At the point of this decision, the plant was still in Configuration 4. If we return to the PSA results for this configuration, we can obtain information as to what is important (i.e., which systems or components) to the prevention of core damage. We can obtain this information in a variety of ways. For example, we could focus on the importance measures such as Fussell-Vesely or RAW. We could also evaluate the accident sequences themselves to see which ones (from the sequences the plant is currently on) lead to core damage. We could also just look at the dominate cut sets for this configuration. Or, we could evaluate the sequences that *do not* lead to core damage in order to determine how best to get onto one of these sequences. Note though, for this last option, the PSA is not normally set up to handle the "non-core damage" sequences and would require modification. For the trial application discussed in this report, we choose the first option, evaluating the importance measures, to glean information on the incident and decision alternatives.


INITIATOR LOSS OF MFW
IE-T2
REACTOR PROTECTION SYSTEM
K
SRV/PORV CLOSES AFTER TRANSIENT
Q-T
AFW
L
SEAL COOLANT FLOW
D3
CCW TO RCS PUMPS
W
CONTAINMENT SYSTEM (CSS, ISR, OSR)
D2
PORVs OPEN FOR FEED & BLEED
P
CONTAINMENT SYSTEM (CSS, ISR, OSR)
CS
CORE VULNERABLE TO DAMAGE
CV
LPR
H1
HPR
H2
"Moving Back" on the Event Tree
Operator Decision-Point
at Time = 9 min

#	SEQ-NAMES	ES-NAMES
1	T2-1	OK
2	T2-2	OK
3	T2-3	CM
4	T2-4	OK
5	T2-5	CM
6	T2-6	T2LH1
7	T2-7	OK
8	T2-8	CM
9	T2-9	CM
10	T2-10	CM
11	T2-11	T2LP
12	T2-12	T2LD2
13 T	T2	FT2T
14 T	T2	FT2TK

Figure 2. PSA representation of Davis-Besse event illustrating the concept of "moving back" on the event tree in PSA space.

Looking at the importance measures for Configuration 4, it is obvious that two items are of interest. First, the ability to utilize feed-and-bleed cooling, even though we have not lost AFW at this point, is of high importance. Second, the availability of AFW is of high importance. Notice that at this decision point in the scenario we did not consider feed-and-bleed to be a viable option. It is not necessary to utilize feed-and-bleed unless all other feedwater alternatives are unavailable. So, using the PSA to provide decision alternatives may result in more alternatives than what would normally be considered. This "feature" of the PSA is not necessarily a negative aspect from the point of invalidating the results. Even if we had kept the alternative of feed-and-bleed cooling at a time of six minutes, the formal decision making evaluation (discussed in the next section) would have demonstrated that going to feed-and-bleed at this juncture of the incident is a poor decision. Keeping the (poor) alternative of going to feed-and-bleed simply complicates the decision-making evaluation.

At a time of 9 minutes, the critical decision faced by the operating crew (and, again, ultimately decided by SRO1) were:

Decision A | t = 9 min	Wait for restoration of the AFW system
Decision B | t = 9 min	Initiate feed-and-bleed cooling

At the point of this decision, the plant was now in Configuration 5. If we return to the PSA results for this configuration, we can obtain information as to what is important (i.e., which systems or components) to the prevention of core damage. Again, for the trial application discussed in this report, we choose to evaluate the importance measures to glean information on the incident and decision alternatives.

Looking at the importance measures for Configuration 5, we see that again we have two items of interest. First, the ability to utilize feed-and-bleed cooling is of high importance. Second, the availability of AFW is of high importance. During the actual plant incident, SRO1 decided to wait for restoration of the AFW system, even though he was advised to begin feed-and-bleed cooling by both RO2 and SRO2. One bit of information that is vital here that we do not get from the PSA (as it is currently implemented) is the timing considerations involved in operation of the NPP. To make the decision between waiting for restoration of AFW or going to feed-and-bleed, one would need to know information such as:

S Time available until feed-and-bleed cooling, if initiated, would still not be sufficient to prevent core damage.

S Time for expected restoration of the AFW system

S The time allowance (i.e., delay in core damage) that was obtained by the action of SRO2 to begin using the startup feedwater pump.

This type of information would be of vital interest in the formal decision-making portion of any incident management system. Note though that the PSA does, again, correctly suggest decision alternatives even though it does not provide timing information specific to the incident. Fortunately, through a combination of probabilistic models and thermohydraulic calculations, the relevant timing information should be available.

We have now evaluated the entire scope of the Davis-Besse incident with respect to the PSA. A summary result of the PSA CCDP calculation is shown in Figure 3. It is important to note that the critical decision points in the incident also coincide with large *increases* in CCDP. We believe that looking for these increases in CCDP may be a very effective method of utilizing the PSA to focus on decision alternative at critical points during an incident. This point is further illustrated graphically via Figure 4.

Further PSA analysis focused on the changes in importance measures (e.g., Fussell-Vesely and RAW) as a function of time. For each configuration, it is possible to calculate and store the numerical value of the importance measures for each basic event in the minimal cut sets. Since the minimal cut set change from configuration-to-configuration (hence, a function of time), the overall importance measures will change. This varying “importance” of components will be vital information to the decision-maker since this information will help to guide where and how to focus resources through the incident.

An illustration of the complexity behind changes in the basic event importance measure is shown in Figure 5. In this figure, we plot the Fussell-Vesely importance measure for a handful of events as a function of configuration. Moving from left to right on this figure simply reflects the individual basic events (R, K, T, IE-T3, etc.). Moving “into” the paper on the figure reflects the evolution of the event importance measure in time. Deeper “into” the paper reflects a later configuration (where “File #1" represents Configuration 1, “File #2" represents Configuration #2, etc.). Then, the numerical value of the Fussell-Vesely is shown on the vertical axis. As you can see in the figure, some events have high Fussell-Vesely importance at the beginning of the sequence that eventually drops off to zero importance (e.g., REC-XHE-FO-DGHWS). Other basic events have low Fussell-Vesely importance early on in the sequence and then later become important (e.g., HPI-XHE-FO-FDBLD). Further investigation into the insights of these time-dependencies of importance measures are warranted.

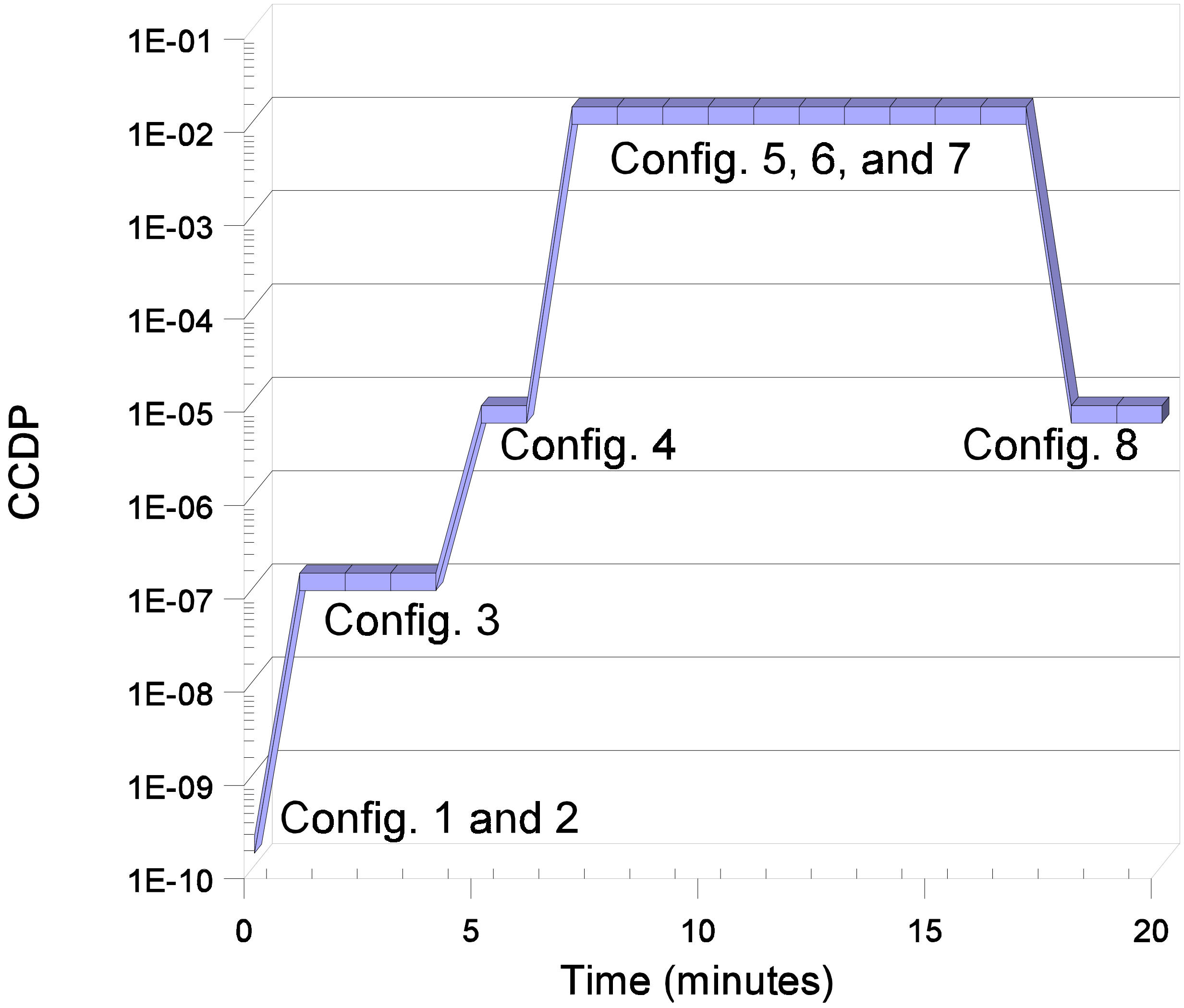


Figure 3. CCDP results for the configurations during the Davis-Besse incident.

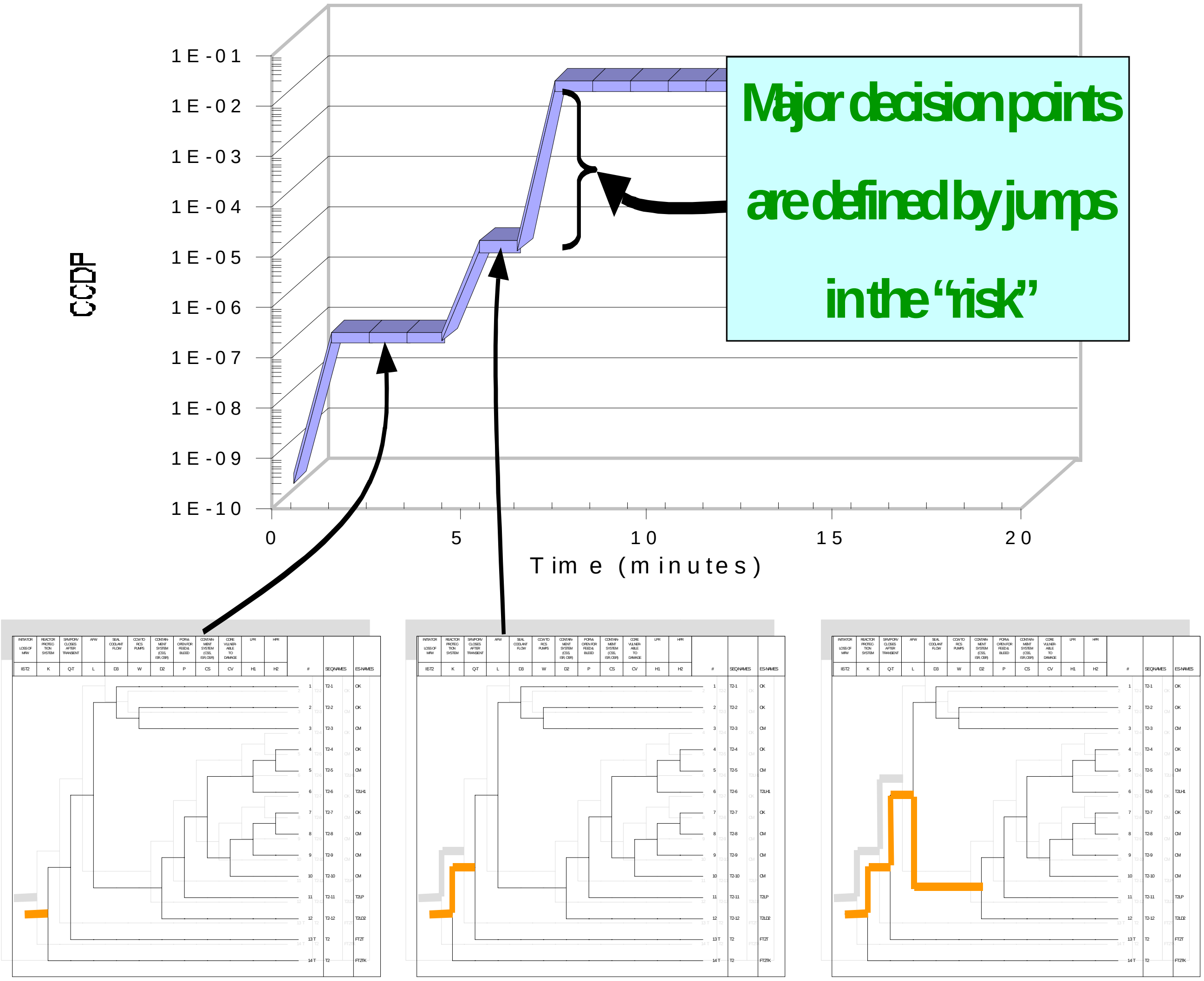


Figure 4. Graphical illustration of the PSA aspect for the Davis-Besse LOOP.

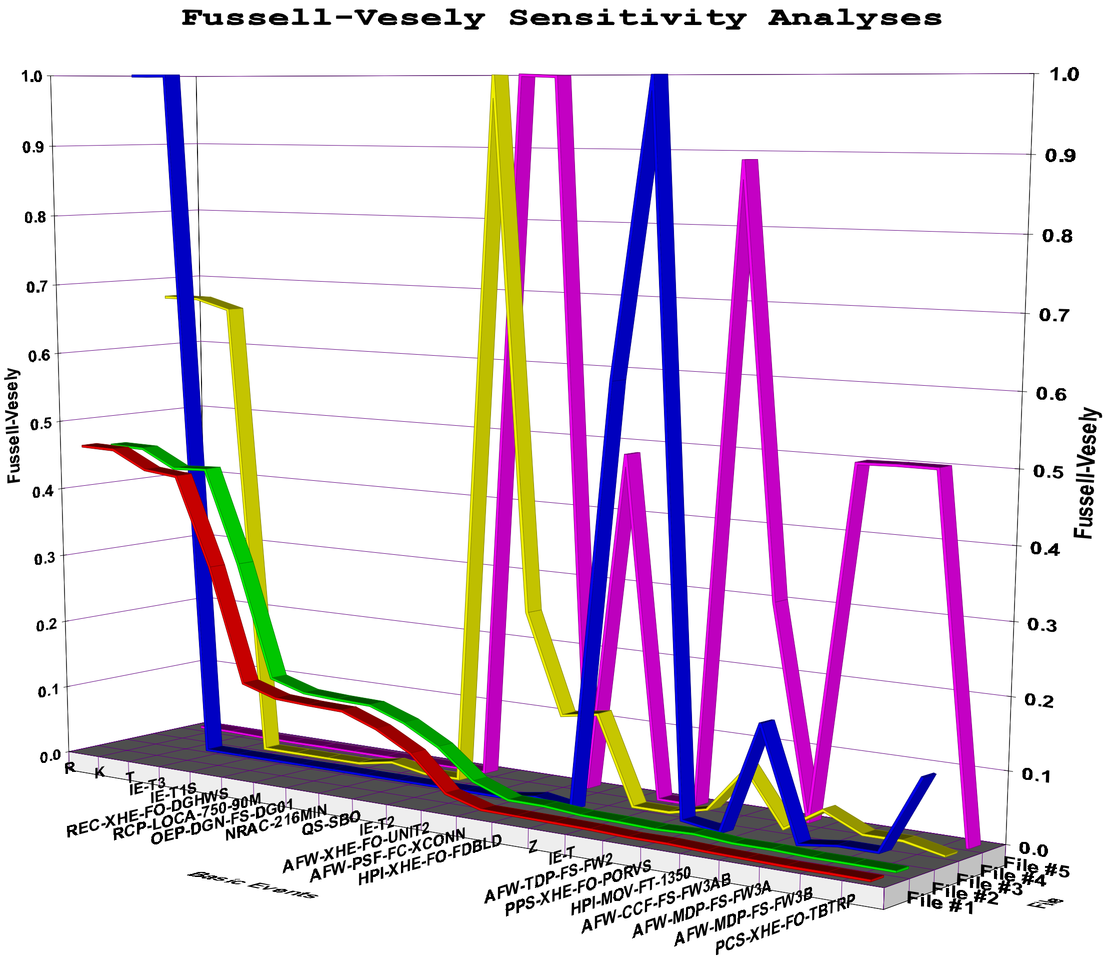


Figure 5. Sensitivity in Fussell-Vesely importance measures as a function of time.

3.2 PSA Analysis for Catawba Loss of Offsite Power Scenario

A preliminary investigation was made into the Catawba loss of offsite power incident. Details of the progress to date are discussed in this section.

To model the Catawba incident, we first had to map the specific event into the PSA model. This mapping process is reflected in Table 7. For this incident, the duration was relatively long and displayed a high CCDP (around 1E-3).

At the time of the initiating event, the critical decisions faced by the operating crew were:

Decision A | t = 0 min	Restore offsite power
Decision B | t = 0 min	Restore diesel generator B
Decision C | t = 0 min	Restore both offsite power and diesel generator B

Later in the incident, operational decision become important. For example, the decision to change modes of power operation (e.g., hot shutdown to cold shutdown) are important. In the decision analysis discussed in Section 4, we address these operational considerations.

After performing the PSA analysis for this configuration (i.e., the loss of offsite power concurrent with the inoperability of diesel generator B) we find that the CCDP experiences a large increase. Thus, this increase is indicative of a critical decision-making juncture. Evaluating the PSA results (e.g., cut sets, importance measures), we see that indeed, recovery of either the diesel generator or offsite power is vital at this point in the incident. These results are summarized in Table 8.

Special attention should be placed on the modes of plant operation that were evident during the incident. The incident started at full power, but eventually the plant was moved to hot shutdown and cold shutdown. The operational decisions to move the plant through different modes is reflected in the CCDP calculation performed for this event.

Table 7. PSA configuration parameters for the Catawba LOOP incident.

Configuration	Time (min.)	Adjusted PSA components	Notes
1	0^-	none	Baseline calculation

2	0^+	E1B = 1.0
		IE-T1 = 1.0
		OEP-CCF-FS-DG12 = 3.2E-2
		OEP-CCF-FS-DG123 = 3.2E-2
		OEP-CCF-FS-DG13 = 3.2E-2
		OEP-CCF-FS-DG23 = 3.2E-2
		OEP-DGN-FR-6HDG2 = 1.0
		OEP-DGN-FR-DG02 = 1.0
		OEP-DGN-FS-DG02 = 1.0
		OEP-DGN-MA-DG02 = 1.0
			The LOOP initiator is set to a value of 1.0 since it was not recoverable.
			Several of the common-cause failure events were set to a value of β (3.2E-2) to represent partial failure of the diesel generator system.

3	180	IE-T1 = 1.0	Recovery of DG-B

4	329	IE-T1 = 1.0
		AFW-TDP-FR-2P24H = 1.0
		AFW-TDP-FR-2P6HR = 1.0
			Isolation of turbine-driven AFW pump

5	975	IESDLOOP = 1.0	Move to hot shutdown model
6	1712	IESDLOOP = 1.0	Move to cold shutdown model

Table 8. Results of the PSA (Catawba) conditional upon configuration 2 (truncation of 1E-10).

Metric	Results for Configuration 2		
Summary Risk Results			
CCDP	1.7E-3		
Sequence Risk Results			
Sequences with the largest absolute frequency	FT1SB	06	SBO-SLOCA2 DOMINANT SEQUENCE RCP SEAL LOCA
	FT1SB	15	SBO-SLOCA2 DOMINANT SEQUENCE RCP SEAL LOCA
	FT1S	08	SBO-SLOCA DOMINANT SEQUENCE RCP SEAL LOCA
	FT1S	04	SBO-BATT DOMINANT SEQUENCE SBO BATT DEPLETION
	FT1S	20	SBO-L DOMINANT SEQUENCE AFW FAILURE
	FT1S	19	SBO-SLOCA DOMINANT SEQUENCE RCP SEAL LOCA
	FT1SB	16	SBO-L2 DOMINANT SEQUENCE AFW FAILURE
	FT1S	15	SBO-BATT DOMINANT SEQUENCE SBO BATT DEPLETION
	FT1S	22	SBO-Q DOMINANT SEQUENCE STUCK OPEN PORV
	FT3	15-08	TURBINE TRIP WITH MFW
Basic Event Results			
Basic events with the largest Fussell-Vesely importance measure	REC-XHE-FO-DGHWS	5.871E-001	OP FAILS TO REC A DG FM HW FAIL IN 3 HR
	RCP-LOCA-750-90M	4.863E-001	750 GPM RCP SEAL LOCA AT 90 MIN
	NRAC-216MIN	4.732E-001	NON-RECOVERY AC PWR W/IN 216 MIN OF LOSP
	OEP-CCF-FS-DG123	3.408E-001	CC FAIL TO START ALL 3 DGS
	OEP-DGN-MA-DG02	3.215E-001	TEST AND MAINTENANCE ON DIESEL GENERATOR 2
	QS-SBO	3.020E-001	POWER CONVERSION SYSTEM: STM GENERATOR INTEGRITY
	OEP-CCF-FS-DG13	2.448E-001	CC FAIL TO START 1 & 3 DGS
	NOTDG-CCF	2.389E-001	SUCCESS OF THE THIRD DG AFTER CCF OF 2
	OEP-DGN-FS-DG01	2.051E-001	DIESEL GENERATOR #1 FAILS TO START
	REC-XHE-FO-DGEN	1.946E-001	OP FAILS TO RECOVER A DG WITHIN 1 HOUR
	OEP-DGN-FS-DG02	1.870E-001	DIESEL GENERATOR #2 FAILS TO START
Basic events with the largest Risk Achievement Worth importance measure	V-TRAIN-2	7.753E+002	INTERFACING LOCA FM RCS LOOP 2 TO LPI
	V-TRAIN-1	7.753E+002	INTERFACING LOCA FM RCS LOOP 1 TO LPI
	V-TRAIN-3	7.753E+002	INTERFACING LOCA FM RCS LOOP 3 TO LPI
	HPI-CKV-FT-CV225	1.756E+001	CHECK VALVE CV225 FAILS TO OPEN
	IE-T1S	1.209E+001	LOSS OF OFFSITE POWER
	OEP-CCF-FS-DG123	1.125E+001	CC FAIL TO START ALL 3 DGS
	HPI-CCF-FT-867CD	5.984E+000	COMMON CAUSE FAILURE OF HPI MOVS 1867C 1867D
	HPI-CCF-FT-115BD	4.163E+000	COMMON CAUSE FAILURE OF MOVS 1115B AND 1115D
	NRAC-216MIN	3.795E+000	NON-RECOVERY AC PWR W/IN 216 MIN OF LOSP
	AFW-TDP-FS-FW2	2.514E+000	TURBINE DRIVEN AFW PUMP FAILS TO START

Metric	Results for Configuration 2

Cut Set Results

```
Cut    CutSet   Prob/
No.      %      Freq.     Basic Event                Description
------  -----  ---------  ------------------------   -------------------------------------------------------
     1    7.7   9.9E-005  IE-T1S                     LOSS OF OFFSITE POWER
                          /L-SB12                    FAILURE OF AFW TDP AT UNIT 1
                          NRAC-216MIN                NON-RECOVERY AC PWR W/IN 216 MIN OF LOSP
                          /O                         OP FAILS TO DEPRESS RCS DURING SBO
                          OEP-CCF-FS-DG123           CC FAIL TO START ALL 3 DGS
                          /Q-SBO                     RCS PORV'S FAIL TO  RECLOSE
                          /QS                        SG SRV/PORV STICK OPEN DURING SBO
                          RCP-LOCA-750-90M           750 GPM RCP SEAL LOCA AT 90 MIN
                          REC-XHE-FO-DGHWS           OP FAILS TO REC A DG FM HW FAIL IN 3 HR
     2    7.7   9.9E-005  IE-T1S                     LOSS OF OFFSITE POWER
                          /L-SB12                    FAILURE OF AFW TDP AT UNIT 1
                          NRAC-216MIN                NON-RECOVERY AC PWR W/IN 216 MIN OF LOSP
                          /O                         OP FAILS TO DEPRESS RCS DURING SBO
                          OEP-CCF-FS-DG123           CC FAIL TO START ALL 3 DGS
                          /Q-SBO                     RCS PORV'S FAIL TO  RECLOSE
                          /QS                        SG SRV/PORV STICK OPEN DURING SBO
                          RCP-LOCA-750-90M           750 GPM RCP SEAL LOCA AT 90 MIN
                          REC-XHE-FO-DGHWS           OP FAILS TO REC A DG FM HW FAIL IN 3 HR
     3    4.0   5.1E-005  IE-T1S                     LOSS OF OFFSITE POWER
                          /L-SB12                    FAILURE OF AFW TDP AT UNIT 1
                          NOTDG-CCF                  SUCCESS OF THE THIRD DG AFTER CCF OF 2
                          NRAC-216MIN                NON-RECOVERY AC PWR W/IN 216 MIN OF LOSP
                          /O                         OP FAILS TO DEPRESS RCS DURING SBO
                          OEP-CCF-FS-DG13            CC FAIL TO START 1 & 3 DGS
                          OEP-DGN-MA-DG02            TEST AND MAINTENANCE ON DIESEL GENERATOR 2
                          /Q-SBO                     RCS PORV'S FAIL TO  RECLOSE
                          /QS                        SG SRV/PORV STICK OPEN DURING SBO
                          RCP-LOCA-750-90M           750 GPM RCP SEAL LOCA AT 90 MIN
                          REC-XHE-FO-DGHWS           OP FAILS TO REC A DG FM HW FAIL IN 3 HR
     4    4.0   5.1E-005  IE-T1S                     LOSS OF OFFSITE POWER
                          /L-SB12                    FAILURE OF AFW TDP AT UNIT 1
                          NOTDG-CCF                  SUCCESS OF THE THIRD DG AFTER CCF OF 2
                          NRAC-216MIN                NON-RECOVERY AC PWR W/IN 216 MIN OF LOSP
                          /O                         OP FAILS TO DEPRESS RCS DURING SBO
                          OEP-CCF-FS-DG13            CC FAIL TO START 1 & 3 DGS
                          OEP-DGN-MA-DG02            TEST AND MAINTENANCE ON DIESEL GENERATOR 2
                          /Q-SBO                     RCS PORV'S FAIL TO  RECLOSE
                          /QS                        SG SRV/PORV STICK OPEN DURING SBO
                          RCP-LOCA-750-90M           750 GPM RCP SEAL LOCA AT 90 MIN
                          REC-XHE-FO-DGHWS           OP FAILS TO REC A DG FM HW FAIL IN 3 HR
```

Since the Catawba incident had only one couple of changes in configuration, the CCDP profile for the event is relatively simple. This profile is shown in Figure 6. Again, in the figure, we see a large increase in CCDP, which indicates a critical decision juncture in the incident. One should notice the lengthy duration of the event. Also, the decision points to move the plant to a different mode of operation (e.g., power to hot shutdown) is indicated in Figure 6.

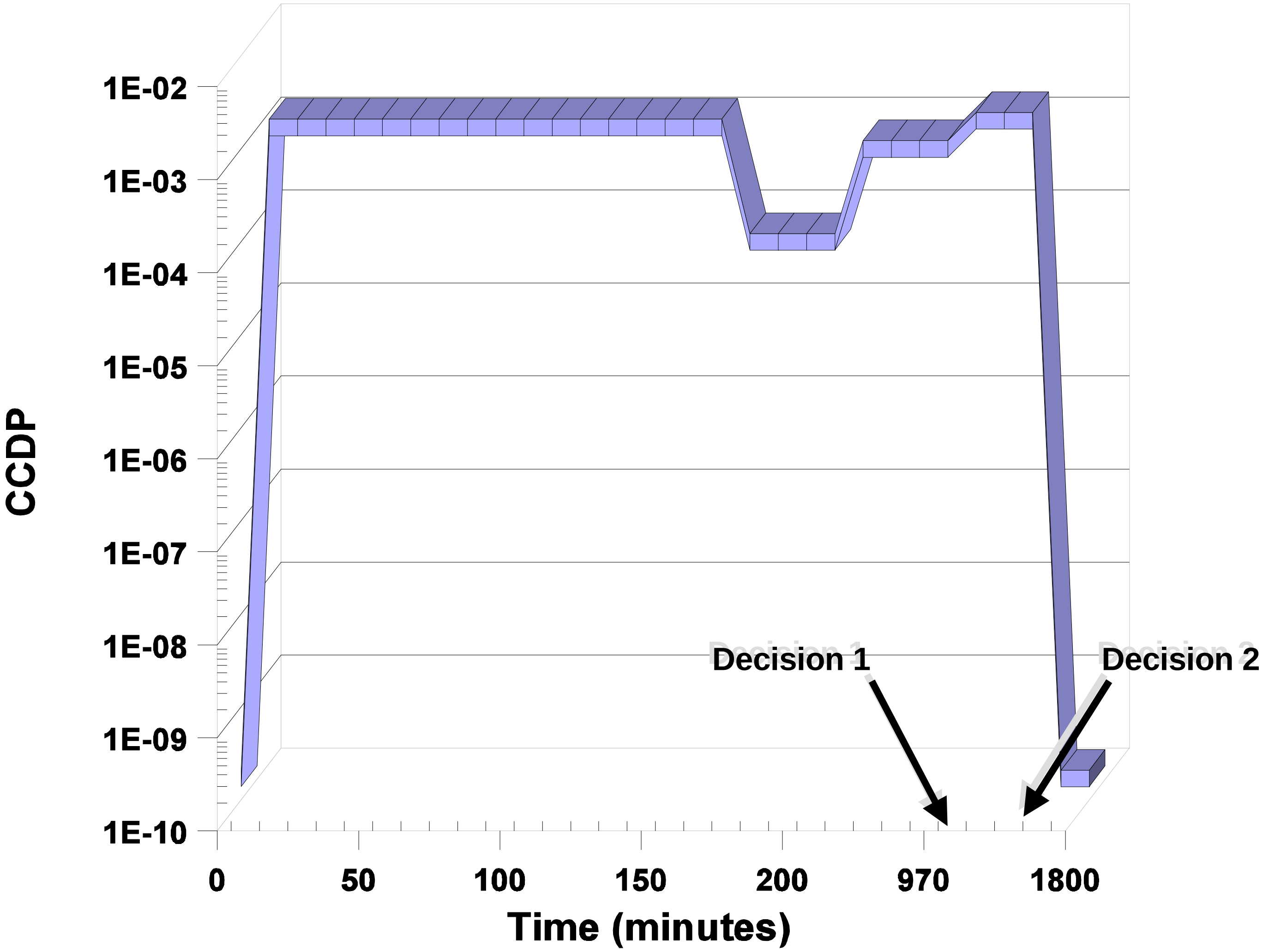


Figure 6. CCDP results for the configurations during the Catawba incident.

Since a PSA model was not available for the Catawba power plant, the Surry 1150 model was used (with the SAPHIRE software) for the at-power modes of operation. For the low-power and shutdown modes of operation, an Accident Sequence Precursor model specifically constructed for low power and shutdown modes was used. This model was constructed by the INEEL for use at the U.S. NRC. This low power/shutdown model was based upon the Surry plant.

The low power/shutdown model contains a reduced list of initiating event in the model (as compared to a full PSA). Fortunately though, a loss of electrical power initiator is included in the model. This initiator represents a loss of either AC or DC power that leads to failure of decay heat removal and/or coolant inventory control. Consequently, the event tree representing this initiating event was used for the Catawba analysis.

Nominally, the low power/shutdown model includes fractions representing portions of time that the plant is in particular modes of operation. For example, POS 2 represents cooldown with the steam generators to a temperature of 345 °F. Based on operational data, this POS will be assigned a fraction that indicates how much timer over the total course of plant operation is actually spent in POS 2. The low power/shutdown modeling activity started with 15 different operating states. These states were grouped into six categories. These categories are:

POS Group 1 Characterized by low power operations and cooldown with the steam generators. This group encompasses the Westinghouse Mode 2 (startup) and Mode 3 (hot standby) operations.

POS Group 2 Characterized by cooldown with the residual heat removal system and cooldown to ambient temperatures. This group includes the Westinghouse Mode 4 (hot shutdown) and Mode 5 (cold shutdown) operations.

POS Group 3 Characterized by draining of the reactor coolant system to mid-loop level (either after shutdown or after refueling). This group includes the Westinghouse Mode 5 (cold shutdown) and Mode 6 (refueling) operations.

POS Group 4 Characterized by operation at mid-loop levels. This group included the Westinghouse Mode 5 (cold shutdown) operations.

POS Group 5 Characterized by refueling activities. This group includes the Westinghouse Mode 6 (refueling) operations.

POS Group 6 Characterized by reactor coolant system heatup. This group includes the Westinghouse Mode 4 (hot shutdown), Mode 3 (hot standby), and Mode 2 (startup) operations.

Since the Catawba analysis was specific to an actual event, we did not use the nominal fractions assigned to each POS. Instead, for each plant state at time t (i.e., for each different configuration), the plant state was known. Thus, we utilized the PSA model to calculate a CCDP that was conditional upon both the component inoperabilities (if any) an the plant state.

An example of the conditional PSA modeling that was used would be for the transition to hot shutdown that occurred at the time of 975 minutes. This new configuration represents being in POS Group 2 in the low power/shutdown model. To model this situation, the POS Group 2 basic event in the PSA was set to a value of 1.0 (while the other POS events were set to a value of 0.0). Then, the analysis is run just like those for the at-power modes of operation.

An example of the level of detail contained in the event tree modeling in the Accident Sequence Precursor low power/shutdown model in contained in Figure 7.

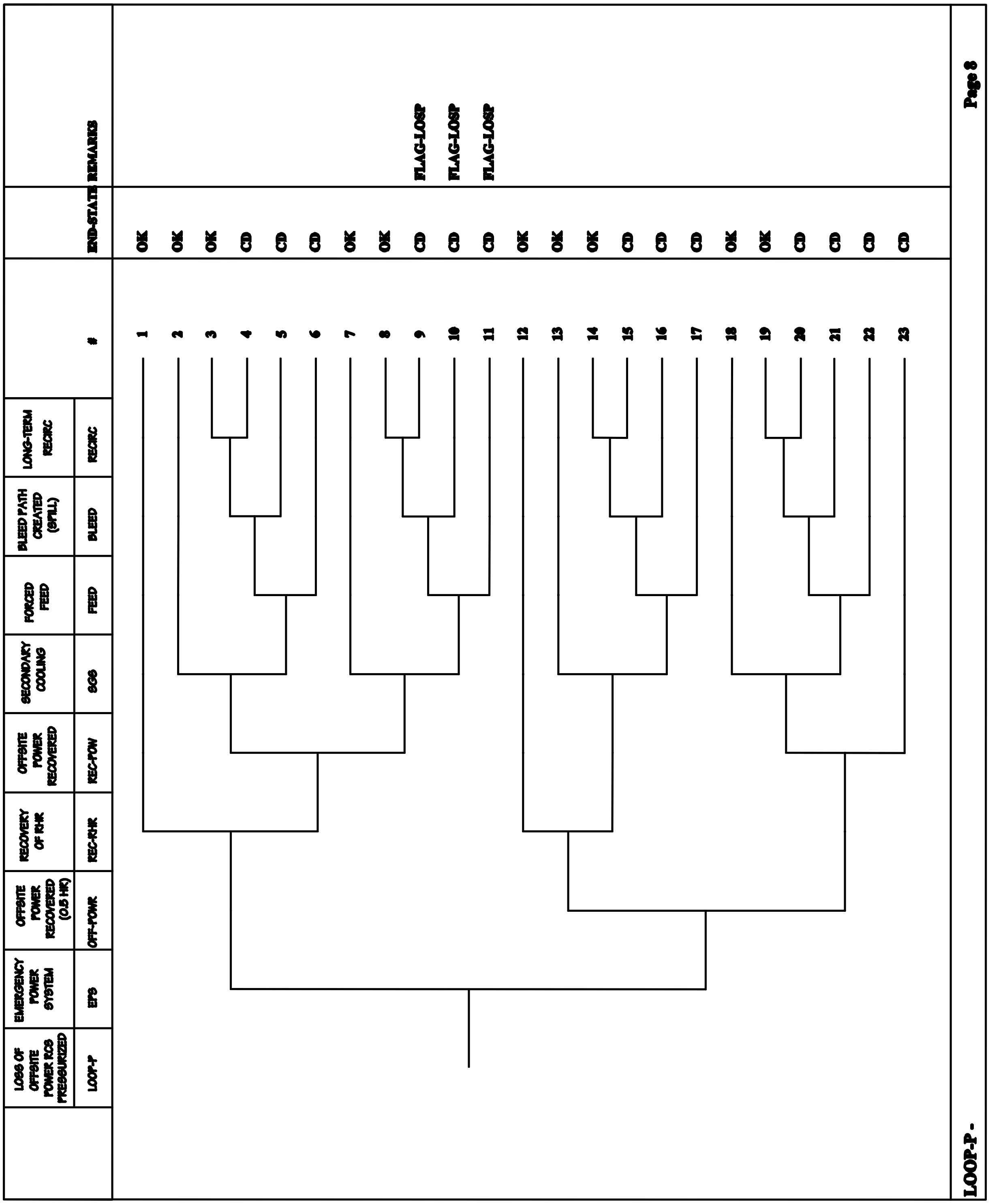


Figure 7. Example of the low power/shutdown loss of offsite power model.

3.3 PSA Application Insights

During the PSA analysis for both the Davis-Besse and the Catawba events, it was evident that several PSA issues would need to be formally investigated and resolved as a part of a incident management system. In this section, we briefly list some of the items that were noted for future research and development.

S During the configuration mapping process when basic events represent failed components, an issue arises with respect to the basic event probability value. Two possible setting can be applied to an event for the failed case: (1) the basic event can be set to a probability of 1 or (2) the basic event can be set to a logical TRUE event. If we set the event to a probability of 1.0, we run the risk of overestimating the core damage probability (due to the Boolean algebra on the minimal cut sets). If we set the basic event to TRUE, the event will get subsumed during the Boolean algebra solution. But, now that the event no longer appears in our cut set results, postprocessing (e.g., recovery rules) of the cut sets are affected. Further, the event's importance measures are not available since the event is not in the cut sets.

S During an incident where redundant components fail, the common-cause failure probability basic event associated with the redundant components must be adjusted to reflect the configuration. Most PSA software tools do not automatically adjust this probability.

S There is a question on absolute importance measure metrics versus relative importance measure metrics. For example, if the RAW for component 1 is 100 (for Configurations 2 and 3) while the RAW for component 2 goes from 2 to 60 (from Configuration 2 to 3), which of these components deserve the most attention during an incident?

S There are several timing considerations to be evaluated as part of the PSA and decision-making process. Examples of these considerations include: coast-down of MFW during initial part of Davis-Besse event, time remaining in incident until feed-and-bleed cooling would not be successful, time that the station batteries would last if Catawba had lost the A diesel generator.

S Since some incidents begin by a plant complication that is not a full-fledged initiating event, we have to deal with both conditional CDFs and conditional CDPs.

S The truncation level for the analysis impacts the basic event importance measures. Consequently, one should determine what is an adequate truncation level for use in an incident management system.

S The aspect of “going back” and moving to “OK” sequences on an event tree was discussed. Normally, the PSA only provided failure cut sets for the “not OK” sequences. Attempting to solve for minimal cut sets for the “OK” sequences complicates the analysis process and slows down the overall analysis time. If it is desirable to have an on-line incident management system, the calculation speed of such as system must be very fast. Consequently, non-traditional calculations (such as solving for the “OK” cut sets) may need to be reviewed to see if the calculation can be optimized.

S Issues related to changes in plant modes of operation will need to be considered. For an incident or operational decision-making framework, the analysis may have to accommodate and use multiple PSA models.

4. THE EVALUATION OF DECISIONS

4.1 Influence Diagrams and their application to an accident sequence: the issue of time dependence in modeling sequential decisions.

As we have illustrated in Task 1 report (Smith, Borgonovo, Apostolakis, 1999), IDs and DTs were introduced in Decision-Analysis mostly for analyzing difficult economical decisions and tradeoffs (Clemen, 1995). IDs offer a simple representation of the logical and probabilistic dependencies among the various events that happen in a decision process. This dependency is graphically depicted by an arc that connects two nodes. The logic of the dependency is captured in the direction of the arrow.

Nodes and Arcs in the diagram refer to probabilistic or deterministic dependencies, but they do not necessarily convey an idea of time ordering. (See Figure 8 for a reference). A causal relationship between two nodes could imply a succession in time. Therefore nodes on the left are generally interpreted as preceding nodes at their right also in a time-dimensional sense, although, time is not an explicit variable of the problem.

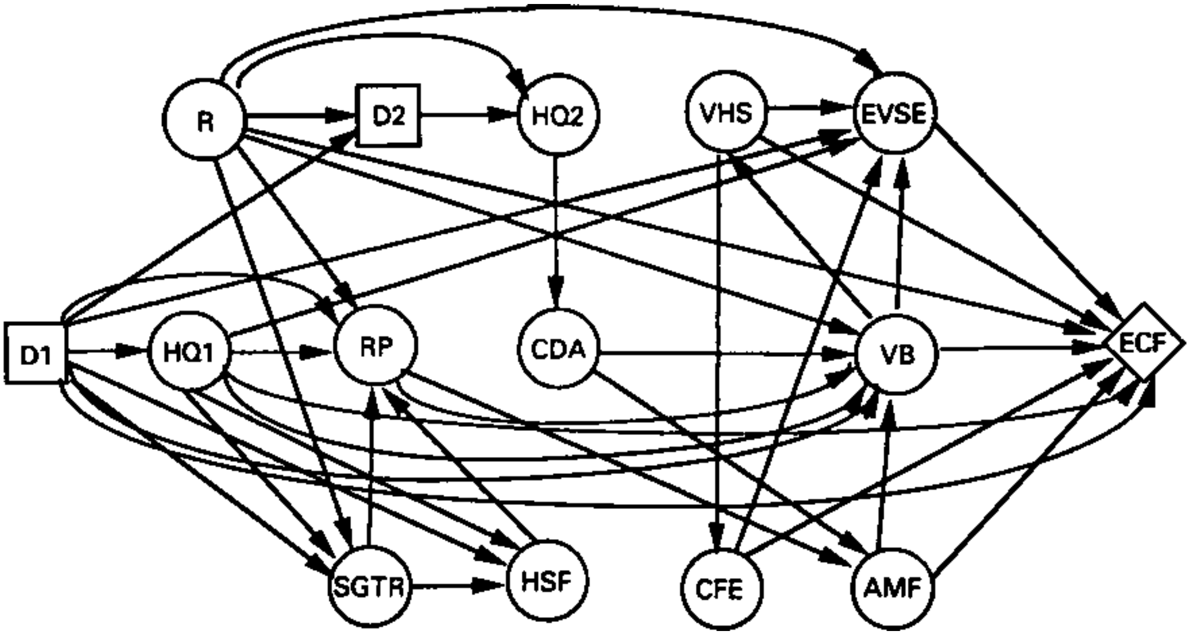


Figure 8. Influence diagram for evaluation of accident management strategies at Surry, U.S. (Jae, Apostolakis, 1993)

For example, in the diagram of Figure 8, we could ask ourselves how much time does the decision maker anticipate exists between the first decision (Node D1) and the second decision (node D2). We can notice that there is no answer to this question: why time does not appear in this diagram? Well, because in this case the analyst has implicitly establish a time horizon for the problem (for example 24 hours), and has approached it as a static problem.

This is not really the way the decision maker (suppose the shift supervisor) operates in a pre-CD situation, where events happen that change the configuration of the plant and response is needed (see Figure 2) to bring the plant in a safe situation. In a real situation, based on his diagnosis, the Shift Supervisor will locate people and resources to pursue what he thinks is the best strategy (at times, his decision could be dictated by existing procedures, at times by his own idea of what is best for the plant). He will be constantly getting information and reassessing his decision. In a few words: the problem is dynamic.

The decision problem the shift supervisor is facing has an analogous in Decision Theory, the so called "'farmer's problem". Let us now think to the following situation: suppose a farmer has to face he following decision: given the weather of a certain day (day 1) in the winter, he must decide whether to protect the crops with a particular chemical. The chemical is expensive and if the weather will be not too bad during winter he will probably not need to spend money on the chemical to protect the crop. On the other hand, if the weather will be bad and the temperature low enough, he will probably loose part or all of the crops. His cash flow will be than seriously in danger. He will have to face the problem every day. On day 1, based on the result of:

- The decisions he took the i-1 days before
- The weather forecast for the next day -day i+1
- The weather of day i

he will have to decide whether or not to protect the crop using the expensive chemical.

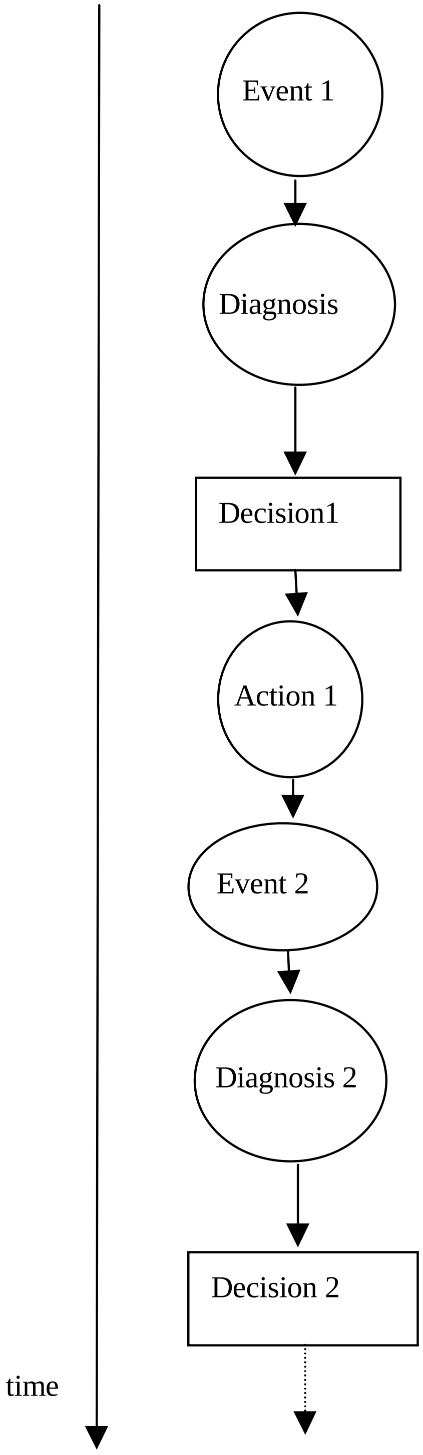


Figure 9: sequential events and decision of an accident sequence.

This kind of decision problem coincides with what is called a sequential decision problem. Influence diagrams can conveniently be used to build a model for this type of situations. As an example, the influence diagram for the farmer's problem is showed in Figure 10.

If we now come back to the situation the shift supervisor is facing during an off-normal plant condition, we can see that the problem is clearly analogous to the farmer's one. In fact, given an off-normal event the shift supervisor will take a decision in response to it. After the decision he will be continuously monitoring the situation, reassessing his decision, and some time after he will have to face another decision problem.

If we now come back to the situation the shift supervisor is facing during an off-normal plant condition, we can see that the problem is clearly analogous to the farmer’s one. In fact, given an off-normal event the shift supervisor will take a decision in response to it. After the decision he will be continuously monitoring the situation, reassessing his decision, and some time after he will have to face another decision problem.

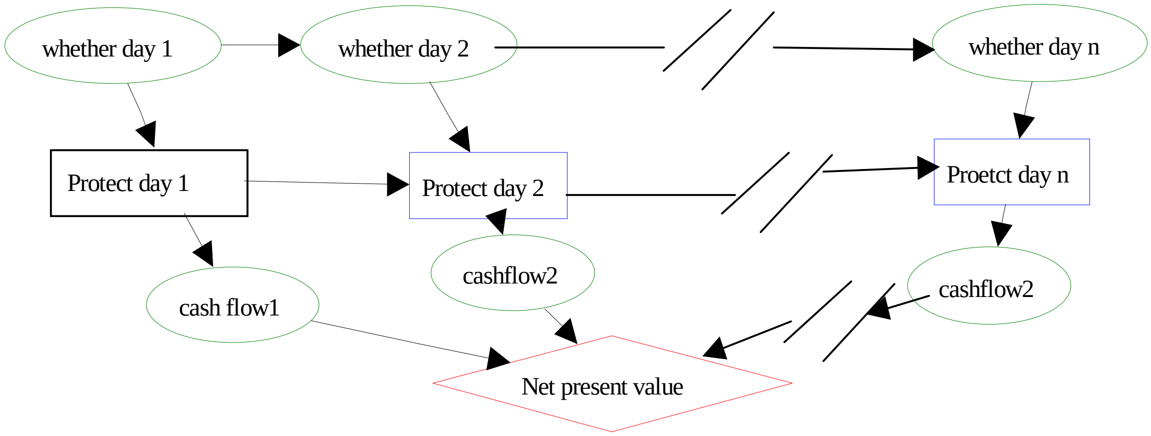


Figure 10. Sequential influence Diagram for the “farmer’s problem” (from Clemen).

Although the “farmer’s problem” is analogous to the “Shift Supervisor’s Problem” with many respects, there are still relevant differences:

S While the structure of the “farmer’s problem” repeats itself steadily,- it is an iterative repetition of the same nodes, corresponding to the same events or variables – the structure of the decision making problem for the Shift supervisor is changing. This implies that each decision will not correspond to the same events, and as an effect nodes between different decision will be different.

S The second main difference is that while for the “farmer’s problem” the time of the different decision is “known” and the time interval between them is also known, this would not be the case in the shift supervisor problem. Sequential decisions will be taken in time intervals that in general will not repeat themselves, but will be strongly dependent on the accident evolution.

S The third main difference is that the decision itself will be changing from a time interval to another. In general after each time interval different possibilities will have to be chosen among by the Decision Maker.

The issue now is how to model these three new aspects in the influence diagram.

The answer relies in a generalized time-displaying influence diagram, in which besides the logical dependence of the events, also the temporal succession is displayed. The generalization of the influence diagram of Figure 11 is straightforward. Instead of day n we will label the node with the foreseen time the decision will be taken. For example 6 minutes, then 9 minutes, then 9 hours, assuming as time zero a convenient time to begin the analysis. This foreseen time may be deduced from actual data (e.g., 20 minutes to restore feedwater on average) or from a engineering evaluation (e.g., thermohydraulics suggest core melt in 30 minutes when all feedwater is lost).

These concepts are summarized in the ID of Figure 11. While this influence diagram refers to the Davis-Besse case study, we show it her for illustrative purposes.. A thorough analysis both of the event and of the ID will follow in section 4.2. Thus, the nodes in the diagram will be explained in Section 4.2. But, for now, note that the ID has nodes with “6" and “9" associated with them; these node represent decisions, events, or conditions in time (6 and 9 minutes, respectively).

A final remark: it is not always necessary to model the decision problem as a sequential influence diagram. In cases of single decisions evaluation a simple probabilistic analysis will be sufficient, as we are to illustrate in the next section.

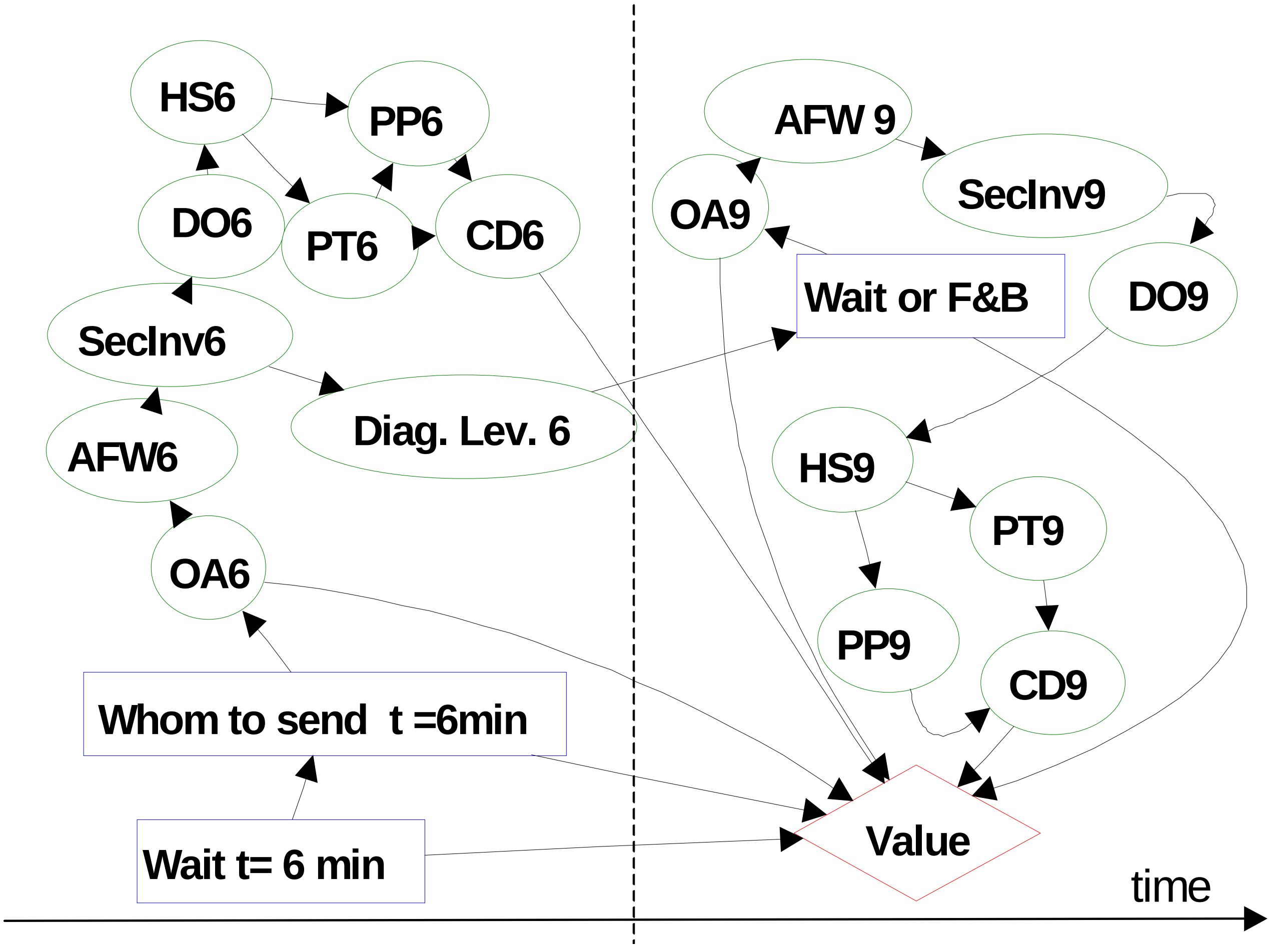


Figure 11. Generalized Time-Displaying Influence Diagram.

4.2 Modeling of Decisions in the Davis-Besse Event

4.2.1: Decisions and Outcomes

As was illustrated in sections 2.1 and 3.1, the main decisions taken by the Shift Supervisor (SRO1) at the Davis-Besse NPP during the accident have taken place at time 6 min and 9 min respectively. A summary of the decisions is displayed in table 4.2:

Table 9: Main decisions in the Davis-Besse sequence

Time	Decision
6 min	Wait AFW
	Start AFW manually
9 min	Wait for restoration of AFW
	Go to Feed and Bleed (F&B)

We know that these two decisions correspond to the two points on the PSA event tree of Figure 1 and that these two decisions are particularly critical because they will decide which path the sequence follow.

Let us look at what happened in the event: a time t = 6 min, the operators decided to start AFW manually. The operator actions failed, causing the unavailability of AFW. At this point, we would be at point 2 in the sequence (right below “Feed and Bleed”). The next decision at 9 minutes has been not to go to feed and bleed (F&B), but to wait for the restoration of AFW.

In the next part of the section we will analyze further the decisions at time 6 min and 9 min, to gain deeper insight on their respective outcomes and options. Let us set us at t= 6 min. Suppose we were to model an incident management strategy. We would have to answer the following questions: given the loss of Main Feedwater: “what were the Decision-Maker options at that moment”? The answer is in table 9. “Was there some other option we have not considered?” The answer is “no”, because at time 6 min the operators did not have to think about F&B, since they had not lost AFW yet.

Let us now try to analyze the driving factors of the decision, both in the form of motives and outcomes, to gain insight on the decision-making tradeoff. One driving factor is certainly the time to core damage (TCD). To gain additional time before CD , we would have to keep a sufficient water inventory in the secondary. The manual actuation of AFW would give us a few minutes of advantage, if successful, with respect to wait for its automatic intervention. Furthermore, if we were uncertain about the conditions of the AFW and we doubt its successful automatic actuation, this gain in time could give us the benefit of some other corrective action. Nonetheless an error in the actuation would cause us to jump one step further in the accident sequence and we would have to face the difficult decision of waiting for the restoration of AFW or to go to F&B.

At time t=9 minutes the decision is, therefore: do we still wait for the AFW system to start or do we have to go to F&B? Here the tradeoff of the decision is more stringent. Hesitating could cause core uncovery, and hence core damage, turning the incident into an accident (with its economic and safety losses). On the other hand, if the AFW turns out to be available, we would be able to bring the plant to a safe shutdown, without economic losses, beside the few days of shutdown. But, going unnecessarily to F&B would expose the plant to an undue economic loss and could cause an extended plant shutdown.

In this decsion, we really see the root of the decision: safety versus economics. Which of the two attributes has to be preferred? Is really F&B a safer solution than wait for AFW? To answer this question in a predictive mode, a methodological approach to the analysis of such decision is necessary (hence, the need for this project). In our case study, what happened was that the operators decided to wait, AFW was finally recovered, and the plant was brought to a safe state.

4.2.2 Decisions in the PSA space

We have already mention in section, that the main decisions for the Davis Besse event can be individuated on the corresponding Event Tree, as seen in Figure 1. Point 1 represents the first decision at 6 minutes. This branch point on the event tree is used to bifurcate the sequence where the up branch indicates success of AFW while the down branch indicated failure of AFW.

Point 2 on the event tree represents the second decision at 9 min. Its implications in PSA space is twofold: (1) we would like to go back to point 1 if possible (notice that, as it is represented, the PSA model does not allow for this possibility) and (2) we would like to jump onto any success path following point 2.

4.2.3 Decision representation for the Davis-Besse event: influence diagram and corresponding decision tree.

We will now represent the main decisions of the Davis-Besse Event in the form of an ID, as explained in section 4.2.1, and show the corresponding DT. This would allow us to prove that a sequential decision problem, with its various events and decision, is effectively represented through a "time-displaying" influence diagram (e.g., Figure 12), and that the corresponding DT can enable us to evaluate the decisions, hence formulating an incident management strategy.

After 6 minutes, the shift supervisor (SRO1) was informed by the secondary reactor operator (RO2) of the possibility to start AFW manually. SRO1 decided to send RO2 to auxiliary feedwater control panel. Strictly speaking, from a modeling point of view, this corresponds to two sequential decisions in a short time. They can be represented by two rectangular nodes on the influence diagram. The arc between the two nodes symbolizes the fact that the second decision depends on the first. If we decide to wait for automatic intervening of the AFW, we do not have to decide whom to send. Now, each of the two decisions involves some operator actions to be started at time t= 6 min (OA6) (in general such a node will always be the one following a decision in an influence diagram for an accidental sequence). Now, it is not certain whether or not the operators will perform their actions correctly. Hence (OA6) is a chance node. It represents the event: "The operators will perform successfully their actions", and its associated parameter is the probability of no error. If we were to be evaluating a decision in a predictive mode, that probability would have to be computed by a human reliability analysis. Important tools like MERMOS would be appropriate to help in the evaluation.

The success or failure of the operators to perform their task will influence the status of the AFW. (In reality they disabled it). Hence the condition of the AFW is not certain. This condition depends on the failure on demand or failure while in standby potential and on the result of the operator actions. The chance node AFW6 represents the event: "Probability of recovery of auxiliary feedwater". The corresponding parameter in our model will be the probability of AFW available, conditioned by the result of node OA. Continuing in our model, the next random factor is the level of water in the Secondary. Obviously the Inventory will be high with a very high probability if we recover AFW, and vice versa. Node SecInv6. The Secondary Inventory will in turn influence the Dry-Out Event DO6, whose probability will be inversely proportional to the Secondary Inventory, and this will go all the way through to Core Damage (CD6) depending on the Heat Sink available (HS6), the value reached by the Primary Pressure (PP6) and Primary Temperature (PT6). All what happens after the decision taken at time 6 min will be monitored by SRO2. In particular, he will be looking at AFW and the Secondary Inventory level. His diagnosis of the situation will influence his next decision: at time t=9 min, he will face the problem of whether to wait for the restoration of AFW or abort this strategy and go to Feed and Bleed (F&B). Now, the best option of the decision at time t= 6 min (his first decision) will depend on the outcome of this second decision at time t=9 min. The outcome of

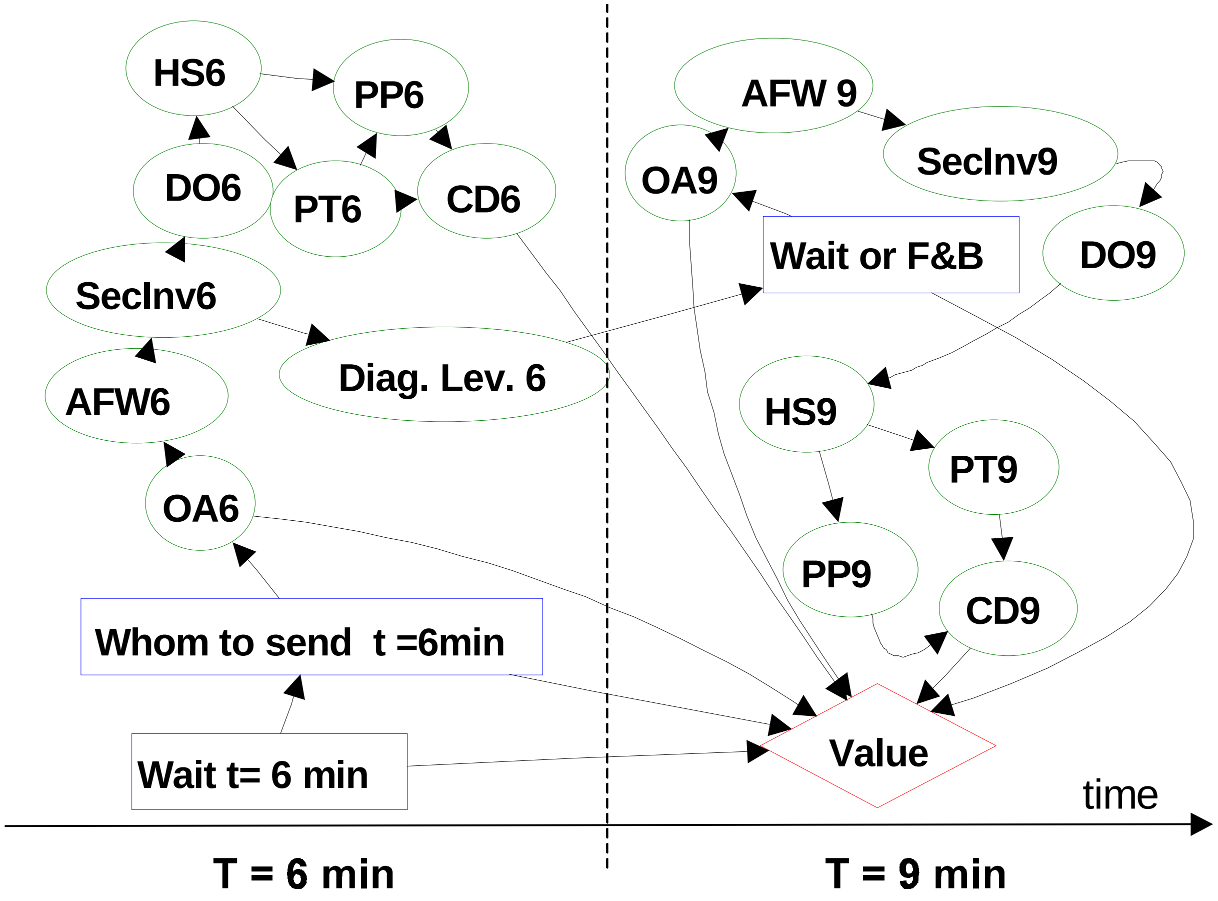


Figure 12. Generalized time-displaying ID.

this decision will influence the operator actions to be taken after 9 minutes (OA9 – with another associated probability depending on the decision at 9 minutes). These will in turn influence the probability of AFW being available after 9 min (AFW9), which will in its turn influence Secondary Level (SecInv9), Dry-Out (DO9), Heat Sink (HS9), Primary Pressure (PP9), Primary Temperature (PT9) and Core Damage (CD9), analogously to what we have seen before. Connecting all the nodes to represent the various dependencies, we obtain the ID depicted in Figure 12.

Let us now refer to the decision at time t = 9 min. We are at t = 9 min, AFW is not working. The dilemma is: to go or not to go to F&B. The time to core Damage is an important factor here. There is a certain time (let us call it $T_{F\&B}$) after which, with no AFW recovery, even performing F&B will not be able to avoid core damage any more. This is the last important decision the Shift Supervisor has to make. Suppose that we decide to let this the last decision of our sequence. – in other words, there are no other decisions to follow this one. Suppose now we want to formally evaluate this decision. We could build a corresponding ID (right side of Figure 12) or we could simply evaluate the decision from a probabilistic point of view, just considering the consequences of each decision and performing a probabilistic calculation. In other words, if the problem contains a single decision, it could not be necessary to go all the way through to the ID representation, but a probabilistic calculation could serve the scope.

As can be noticed, this ID offer a compact representation of this very complex probabilistic problem. Nonetheless, it is not immediate to have a picture of the resulting sequence in all its bifurcation only looking at this diagram.

To overcome this issue, it is possible (with the appropriate software) to use a DT representation (Apostolakis, Borgonovo, Smith, 1999). This would also enable the analyst to perform corresponding calculations and sensitivity analysis to corroborate the model (For this part, see appendix B).

We will now illustrate the DT corresponding to the ID of Figure 12. As illustrated in our report on Task 1, a DT is a graph whose elements are: nodes (Decision and Chances) and Branches which connects the various nodes. Each branch corresponds to a different outcome of a chance node or of a decisions. The first node of any DT represents the first decision (rectangular node in Figure 12). The node defines the decisions, which, as we know, consists in the choice between different options. In our case we have to choose between the alternatives

1. Wait for automatic actuation of AFW

2. Start AFW manually

These options obviously coincide with the ones we represented in the first decision node of the ID.

Since we have two alternatives, two branches will emanate from the first node. In fact, operator actions , systems influenced by the decision and, hence, future events, will depend on the decisions we have taken. Let us now follow one path in the DT, and namely, the path that happens if we decide for the first alternative (to wait). Looking at the ID of Figure 12, we see that the first element influenced by our decisions will be the set of Operator Actions they have to perform in case we decide to start AFW manually. In our ID of Figure 12 this was represented in node OA6, that we know is the event: "Operators will perform the requested action successfully". If we decide to use a binary logic, that is to say: Operators will be either successful or unsuccessful (error) two branches will emanate from node OA6. If Operators will perform the required action correctly then we will follow the lower branch of Node OA6, namely No-Error, otherwise we will climb our tree through the upper branch Error. Now, there will be a certain probability that the operators will be successful and a certain probability of failure to perform the required actions (indicated as 1 - peaw6 and peaw6, respectively) . From the ID of Figure 12, we know that operator actions will in turn influence the availability of the AFW system, whose probability of being available is conditional to their performance (pafwav6e, representing the probability AFW available given an error). Hence the next node in the tree will be the event the Auxiliary Feedwater system will be available at t=6 min. These nodes are illustrated in the DT in Figure 13. Again, assuming a binary logic for this event, we will add two more branches, namely Available and Unavailable.

We can continue modeling the DT by adding the nodes corresponding to the ID of Figure 12, until we come to the second decision node. We know that this decision will be taken after the diagnosis of the level of the secondary inventory. The decision options are:

S Wait for recovery of AFW
S Go to F&B

These items can be seen in the DT in Figure 14.

We know that the decision at 9 min will be taken after a certain time from the first decision. Based on the analysis of the event, we set the time interval to be equal to 3 minutes. One of the challenges of the methodology we are developing will be the time-parameterization of the sequence.

Continuing to follow the branches, suppose AFW available, and diagnosis, we would be on the decision node "Wait or go to F&B". Each of the two decision options will in any case imply Operator action at 9 minutes or more. If we decide to wait and allocate resources to recover AFW, the outcome of these actions will influence the availability of the system analogously to the situation at 6 minutes. Finally the availability of AFW will influence Core Damage[1].

At this point the tree ends, and we have the Value node of the tree. This node represent a quantification of the consequences of the outcomes. It can be money, or in general, according to classical Decision Theory, a Utility function established by he decision maker. The strategy (sequence of decisions) that maximized this utility will be the best strategy.

[1] It can be noticed that we go here directly from node AFW9 to CD, and, with respect to the influence diagram of figure 4.5, we have eliminated nodes SecInv9, HS9, DO9, PP9, PT9. The reason is that all these dependencies con be summarized in only one node (node CD9) , and taken into account when calculating the probability corresponding to the node.

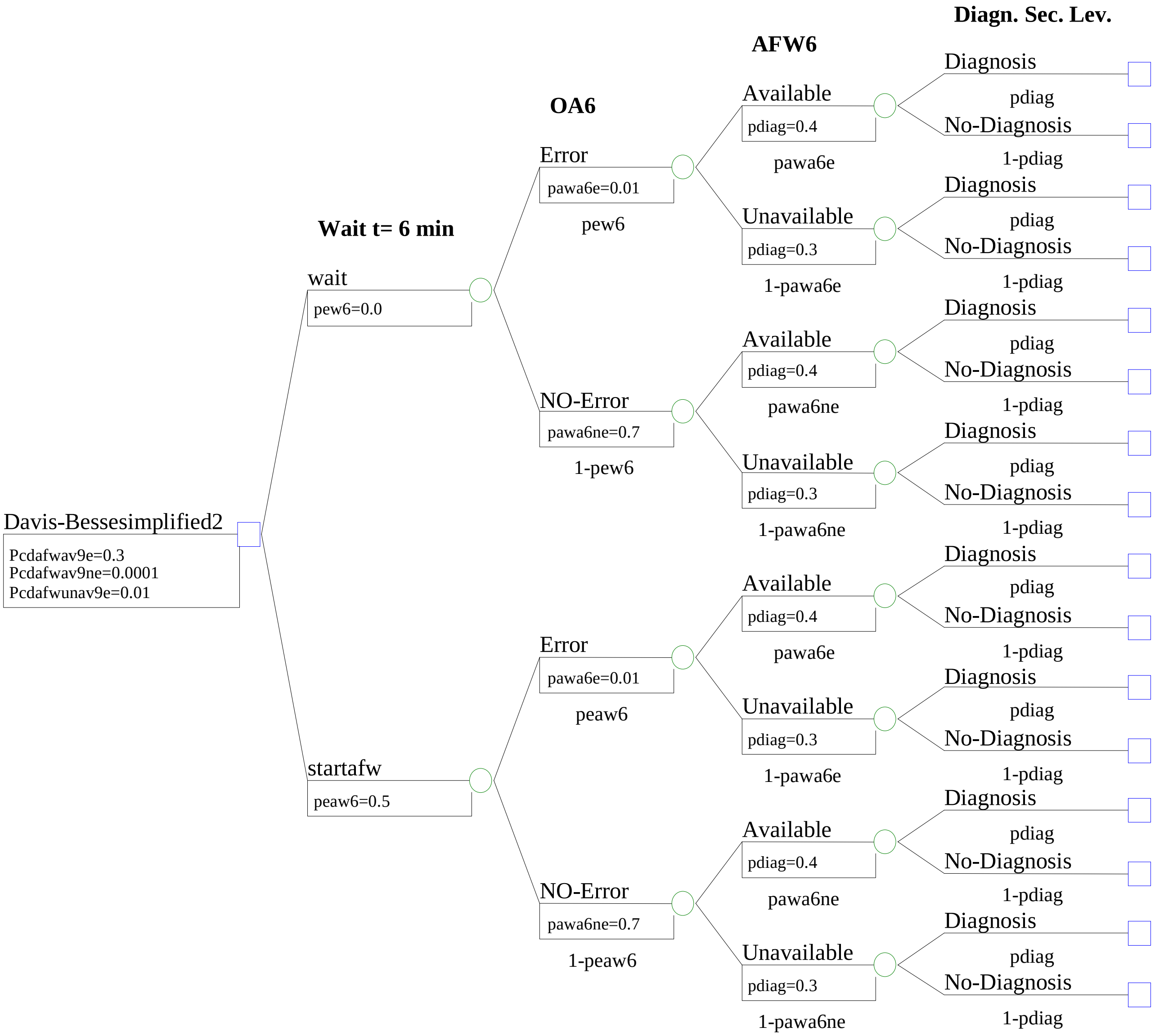


Figure 13. First branches of the DT of ID from Figure 11.

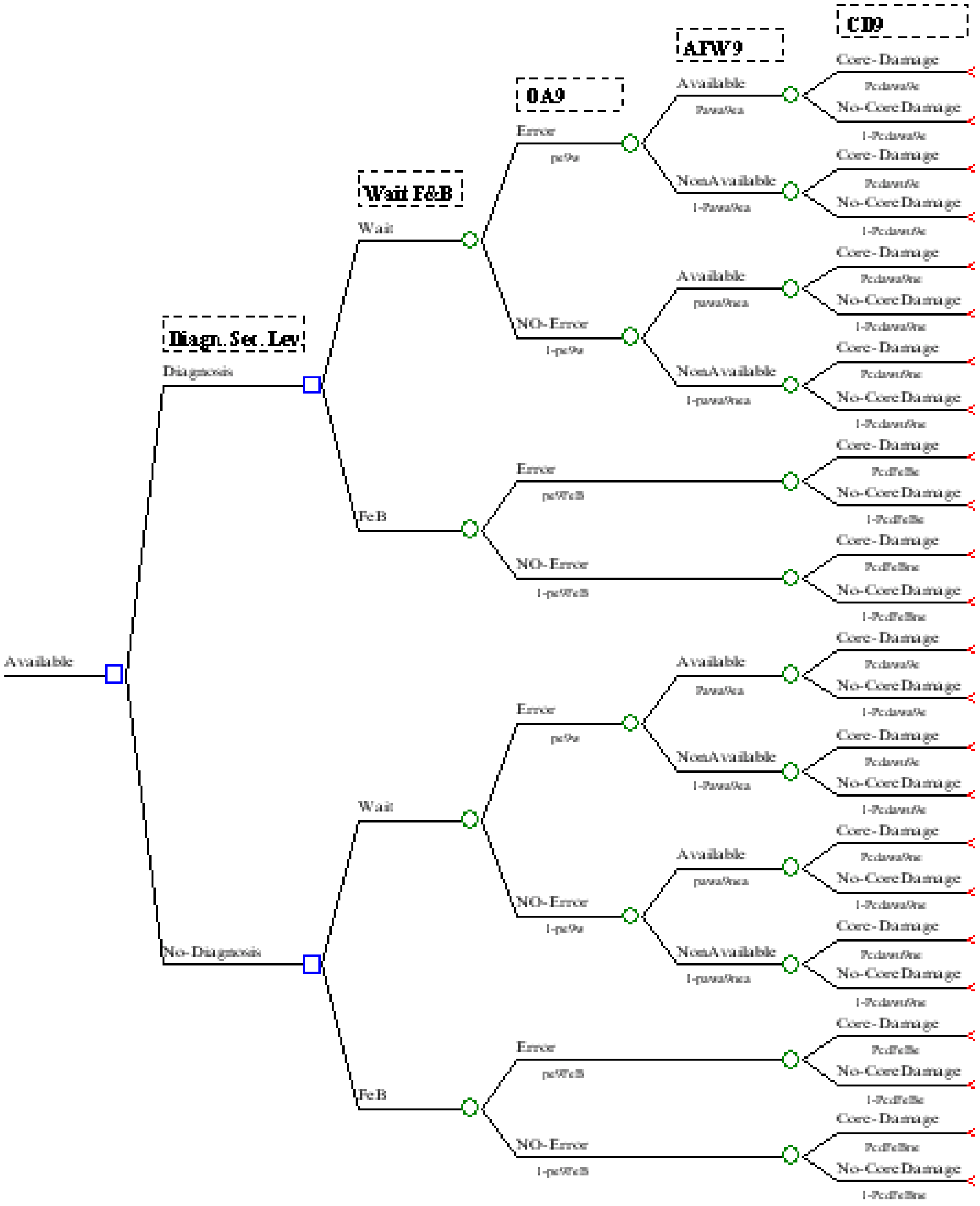


Figure 14. Last branches of the DT corresponding to the ID of figure 11.

One is now curious to know, what would have been the best strategy based on this “a posteriori analysis”. Well, we decided to pursue this further. We used a very simple utility function for the outcomes: if we have core damage we would have a negative 1 (-1), in case we avoid core damage we would gain a +1. Based on probability values assigned according to our calculations and judgment we found the following interesting result:

> At time 6 minutes the best decision would have been: “wait”. In case we would have waited, given that AFW was available at 9 min, at 9 minutes the best decision would have been to wait. If AFW would have been unavailable at 9 min, the best decision would have been in any case to go to F&B. This is what the NRC would have liked the operators to have done in that situation. What the operators did in reality was different. The difference mainly rises from the utility function we used. We used here a conservative, risk-averse, utility function. This type of utility prizes only safety and not economics, which is what a regulatory body wants. The decision of the shift supervisor not to go to F&B was, however, motivated by economical reasons.[1]

[1] These results are based on an expected value calculation of the best decision. A ore refined way of analysis is presented in appendix A.

4.3 Decisional Aspects of the Catawba Event

At 12:31 in the afternoon, while the plant was at 100% power, ground faults on both main transformers started a loss of offsite power (LOOP). The reactor scrammed very shortly after the LOOP. The plant has two on-site emergency diesel generators (EDGs), EDG-A and EDG-B. Very shortly after the reactor scram, EDG-A started automatically. EDG-B was out of service at the time of the LOOP.

Five minutes after the LOOP, the operators closed the main steam isolation valve. Two minutes later, safety injection (SI) occurred due to low steam pressure in steam generator (SG) A. Eleven minutes later, the reactor coolant system pressurizer power-operated relief valve (PORV) began to open and close. After another 23 minutes, the pressurizer went solid. This situation led to a rupture of the pressurizer rupture disc ten minutes later. It wasn’t until approximately 6 hours later that a steam bubble was restored in the pressurizer.

Repairs on EDG-B were underway at the time of the LOOP. The EDG-B was restored approximately three hours after the LOOP. Partial offsite power was restored to the “B” busses approximately 5-1/2 hours after the LOOP. Additional partial offsite power sources were available to the “A” busses approximately 7-1/2 hours after the LOOP. Full restoration of offsite power was realized around 36 hours after the LOOP.

The scenario is represented by the sequence of events shown below:

Events in time:

0 min	LOOP with unavailability of diesel generator B
5 min	Close MSIV
7 min	SI started
18 min	PORV begin cycling
41 min	Pressurizer is solid
51 min	Pressurizer rupture disc ruptures
180 min	DG-B restored to service
251 min	Leak from TD AFW pump
329 min	TD AFW pump isolated
330 min	Partial restoration of off-site power to "B" busses
470 min	Partial restoration of off-site power to "A" busses
975 min	Hot Shutdown
1712 min	Cold Shutdown
2160 min	Full restoration of off-site power

As can be inferred from the Catawba event description, and as we already pointed out in our previous report (Borgonovo, Smith, Apostolakis, 1999)[1] the decisions taken during the first part of the event, that is during the bulk of the accident, were mainly dictated by procedures. Hence, not much freedom was left to the decision-maker. Conversely, after the reactor was brought to a safe state, safety injection was suspended and natural circulation was initiated, which caused the decision-making aspects from the realm of procedures to the management level. It is on this second phase of the Catawba event that we will focus our attention in the following sections of this report.

Let us now begin with a summary description of the influence diagram that will be explained with more detail in the next paragraphs. We know that, after a LOOP the plant is brought to a safe condition, SI is suspended, and the plant is in the natural circulation (NC) mode. The management must now plan the last phase of the accident. There could be the possibility of bringing the reactor back to power or going from natural circulation to cold shutdown, towards an unplanned outage, depending on plant conditions and the estimated severity of the accident. The first option would be more convenient from an economical point of view, but risky if the conditions of the reactor have been somehow worsened by the incident. The second option would correspond to more severe economical consequences (longer non-production time), but could allow an increased level of inspection and a better post-accident condition evaluation. This, in its turn, could avoid the consequences of the bad publicity and the costs associated with an another unplanned outage. In particular, the complete recovery of offsite power (R) and the availability of the diesel generators play a key role in the last phase of the accident. In fact, if off-site power is recovered and the plant is thought not to have undergone substantial damage, to plan a return to full power could be reasonable. Conversely, if no off-site power is recovered, going to hot shutdown would seem the most logical option.

As it can be noticed, the first decision needs to be accompanied by a second decision after a certain time-interval. In fact, if, for example, we decided to stay further in NC, (this decision was taken at t=975 min) we would have to make another decision, to decide whether to go back to power or go to HS. The actual time of the second decision was 1720 min. A second Decision-Node will then be used in the influence diagram as can be seen from Figure 15. Once we know the conditions of the plant (represented by nodes R=recovery of off-site power, DG=availability of diesel Generators) we can calculate from the PSA model the conditional Core Damage (CD) Probability (CCDP) (the Core Damage Event is represented by Node CD), based also on the decision taken, that is on whether we are in the NC or full power or HS state. The dependency between the nodes will repeats itself after the first decision.

[1] The ID for the complete Catawba Accident can be found in Borgonovo, Smith, Apostolakis, 1999

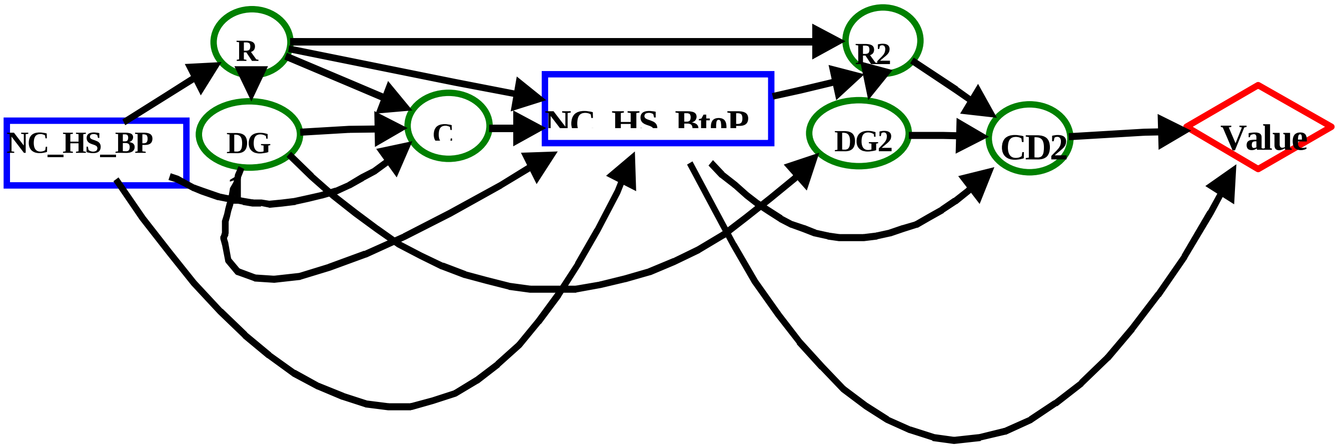


Figure 15: Influence diagram for the second phase of the Catawba event

We will now analyze further the influence diagram for the second phase of the Catawba event, beginning with decision timing and alternatives, continuing with the chance and value nodes. We will then describe the corresponding decision tree structure. Finally we will present and comment on the results of the point estimate, Monte Carlo and sensitivity analysis.

4.3.1: Decisions timing and decision alternatives

For a complete evaluation of the strategy, not only the alternatives of each decision must be established, but also the corresponding times should be addressed and eventually optimized.

This means that, as already discussed in part in the previous progress report (Borgonovo, Smith, Apostolakis,1999), time enters the framework of Influence Diagrams or DTs as a parameter. The way of introducing time dependence in influence diagrams is still an open issue. For the purpose of the present report, we wish to gain information from an event that occurred. So, we will not evaluate the time-optimization problem at this stage (this will be part of the future work of the project).

In the case of the Catawba event, as we already discussed, we have denoted two main decision points. From the chronology of the event it is easy to set these points in time. Hence we will think of decision 1 as to have been taken at time T1=975 min and decision 2 at time T2=1712 min.

Once we establish the time of the decisions, we must delineate the options available for each decision at each time. For the Catawba event, after the first decision at t=920 min, we would have to take another decision to reevaluate the previously chosen strategy. For example, suppose we decided to stay in natural circulation for the first decision at T1. At T_2 we would have to reevaluate this decision to establish whether we could go back to power or we have to go to Hot Shutdown. The decision alternatives are represented in Table 10.

Let us summarize the individuated options and explain the logic of Table 10: after the accident at time T_1 we could decide between: Natural Circulation (NC), going back to power (BP) and going to Hot Shutdown (HS). At time T_2 the decision alternatives will be: staying in NC, choose BP, HS or go to Cold Shutdown (CS). Clearly the options of this second decision depend on the first decision. For example, if at T_1 we decided to remain in NC , at T_2 we could decide between HS and BP, but we would not have the opportunity to go to Cold Shutdown (CS). Analogously, if we decided for option BP at T_1 we could not go directly to HS or CS.

Table 10: Decision Alternatives for the Catawba event

Decision 1	Decision 2
1. Natural circulation	1. Natural circulation
2. Back to power	2. Back to power
3. Hot shutdown	3. Hot shutdown
	4. Cold shutdown

4.3.2: Chance Nodes

Node DG: represents the event: “Diesel generators are available between time T1 and T2”. This chance node has three outcomes: both diesel generators A and B are available at time T1, only one diesel generator is available (A or B) no diesel generators are available.

Node R: represents the event: “Off-site power is recovered between time T1 and T2”. Two are the modeled outcomes, namely off site power is “Recovered” or “Not Recovered”.

Node CD: represents the event: “Core damage happens between time T1 and T2”. Two are the possible outcomes associated with this node, and namely “Core damage” and “No core Damage”. Node CD depends on the current plant configuration, which is dictated by the number of available diesel generators and the recovery of offsite power. It also depends on the strategy selected, because the core damage risk is different in NC, HS, CS or at Power. [1]

Node DG2: represents the event: “Diesel generators are available after time T2”. This chance node has

[1] Clearly other factors could have been chosen to influence CD, like, for example the availability of RHR. They are anyway embedded in the CCDP, and hence representing them or not is more a modeling choice than a real numerical concern.

three outcomes: both diesel generators A and B are available after T2, only one diesel generator is available (A or B) no diesel generators are available. Node DG2 depends on node DG1, in fact the availability of a diesel generator after time T2 is, in general, conditional of its status between T1 an T2.

Node R2: represents the event: "Off-site power is recovered after T2". Two are the modeled outcomes, namely off site power is "Recovered" or "Not Recovered". In this case recovery of off-site power after T2 depends on its recovery between T1 and T2. In fact, if it is recovered at T2 we could assume that it remains recovered also after T2.

Node CD2: represents the event: "Core damage happens after T2". For CD2 analogous considerations hold as for node CD.

4.3.3: Value Node

In every decision making problem, the consequences of each decision alternatives must be determined. Consequences are the result of the random events and actions that correspond to the implementation of a certain decision-alternative. In general, for the nuclear world, the consequences embrace a wide range, going from environment protection to material safeguard. A decision alternative with high core damage probability will pose severe threat on the economics of the plant, as well as impacting workers exposure, public exposure and the environment in case of radioactive release from the containment.

Once the decision-maker has determined the consequences of a certain decision, his attitude would be that of choosing the option that maximizes the positive outcomes and minimizes the negative ones. It is obvious that, in a typical situation, the decision maker will want to minimize workers exposure or regulatory consequences while maximizing profit.

In decision theory, attributes are used that synthesize the link between consequences and objectives. Each consequence and outcome of a decision alternative is associated with a numerical value (attribute). For example, if we have established that the relevant consequences of our decision-making problem are workers exposure and economic loss than the decision will have two attributes: person-rem dose to quantify workers exposure and money to quantify economic loss. The decision-maker will then choose the alternative he judges to give the best with respect to economic loss and workers' safety.

A list of possible attributes (or evaluation criteria) of a decision-making problem for the nuclear industry are given in Table 11.

Table 11: Evaluation criteria

Production Cost
Operational Cost
Plant value
Outside Radiation Release
Workers Exposure
Bad Publicity-- Loss of prestige
Regulatory aspects

For the case of the Catawba event we choose to quantify the decision based on a judgmental utility function (a global loss function) , of the following form:

$$U = \left\{ \begin{array}{l} -1000000 \quad if\ core-damage\, happens \\ \hline -10 \quad if\ we\, are\, able\, to\, go\, back\, to\, power \\ \hline -100 \qquad\qquad if\ we\ stay\, in\ \ NC\, or\, HS \\ \hline -200 \qquad\qquad\qquad if\ we\ go\ to\ CS \\ \\ \\ \end{array} \right\} \ (1)$$

The rational behind U is the following: if core damage we would suffer the greatest loss, and we would assign to it the worst possible value, in this case -1,000,000. On the other side, if we were able to go back to power and suffer no additional damage from the accident, we would have only the monetary loss of the duration of the accident and would quantify it as a minimal loss. In other words, this would be the best situation and we would quantify it as a –10. If , on the other and, we are forced to remain longer in NC or go to HS, we would have intermediate economical losses and we would judge this as –100. If we are forced to go to cold shutdown towards an unplanned outage, we would judge this option as worth –200[1]. [2]

[1] It is perhaps worth to point out here that, as one can notice, some of the options have higher probability to lead to core damage (are riskier). This has been taken into account by the higher values of their CCDP inserted in the ID and DT. However when expressing our preference regarding an outcome, we should judge it independently of its probability.

[2] In general a more complete formalism could be used to establish evaluation criteria for a decision-making problem in the nuclear industry. Since this is beyond the scope of the present report, we will not deal with this problem any further here, but this analysis will be part of the second phase of this project (see also the Conclusions section).

4.3.4: Decision Tree and Variables

The general structure of the decision tree resulting from the Catawba ID can be seen in Figure 16. In this figure, we give a representative view of important portions of the overall tree. Unfortunately, it is not possible to display the tree on one (or a couple) of pages due to its complexity.

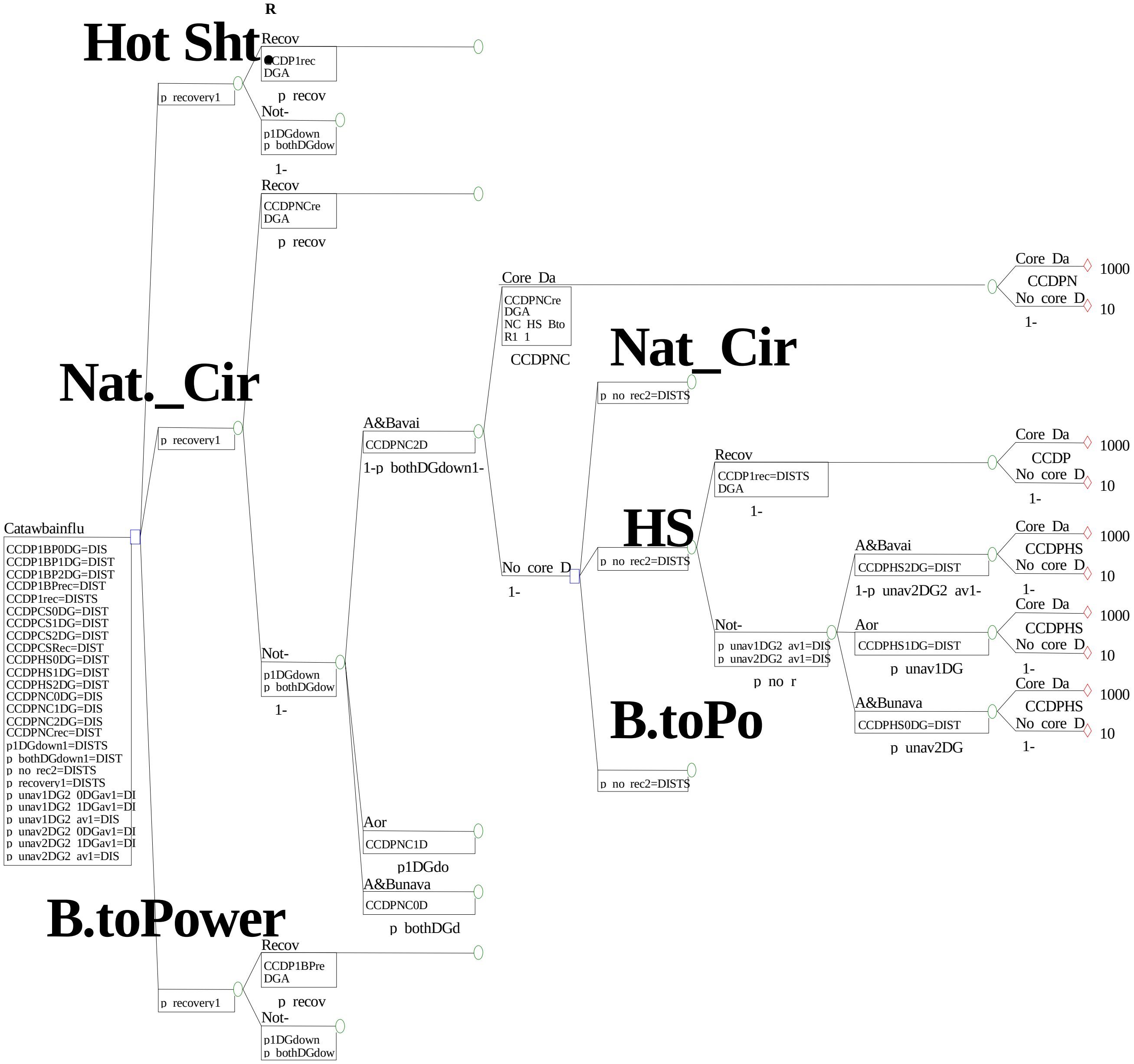


Figure 16: Decision tree structure for the Catawba event

1-

As can be seen, the first decision gives rise to three branches, each corresponding to an available option. Let us now follow a path in the three, to better understand the structure of our model for this decision-making problem. Suppose we choose NC: the first random event we would encounter would be the recovery of offsite power. This node gives rise to two branches. If offsite power is recovered we will go up in the tree, if it is not recovered, we will follow the lower branch. The splitting is determined by the probability of recovering off-site power between times T1 and T2. This probability is described by the variable “p_recovery”. Following the lower branch leads us to the node “Diesel Generators (DG)”. As described previously, three possible outcomes are associated with this node. The corresponding probabilities are given by: p1Dgdown1, - probability that 1 DG is down between T1 and T2 -, p-bothDGdown 1, - probability that both DG are down between T1 and T2 -, and 1- p-bothDGdown-p1Dgdown1.

The next node is node Core Damage. This node has two associated outcomes and the probability of core damage is the CCDP between T1 and T2 given that we are in a configuration individuated by: Natural Circulation with zero, one or two DGs respectively and no off-site power. Clearly if CD happens, we jump directly to the end of the tree, otherwise we can reevaluate the decision taken at T1. Hence following the path no-CD, we meet the second decision node, node NC_HS_BP_CS. We now have four available options, as can be easily understood from the name of the node. In our path, since we choose to stay in NC, we cannot go directly to CS and hence this option is not accounted for in this particular path. After the second Decision Node, the structure of the tree repeats itself till the value node. The complete list of variables names is given in Table 12.

Table 12: List of variables

Variable	Meaning	Point
CCDP1BP0DG	CCDP given we are have chosen to go back to power and no DGs are available	1e-1
CCDP1BP1DG	CCDP given we are have chosen to go back to power and 1 DG is available	5e-2
CCDP1BP2DG	CCDP given we are have chosen to go back to power and 2 DGs are available	1e-4
CCDP1BPrec	CCDP given we are have chosen to go back to power and off site power is recovered	1e-4
CCDP1rec	CCDP given we are have chosen HS and off site power is recovered	1e-5
CCDPCS0DG	CCDP given we are have chosen CS and no DGs are available	1e-3
CCDPCS1DG	CCDP given we are have chosen CS and 1 DGs is available	1e-5
CCDPCS2DG	CCDP given we are have chosen CS and 2 DGs are available	1e-7
CCDPCSRec	CCDP given we are have chosen CS and off-site power is recovered	1e-7
CCDPHS0DG	CCDP given we are have chosen HS and no DGs are available	1e-2
CCDPHS1DG	CCDP given we are have chosen HS and 1 DGs is available	1e-3
CCDPHS2DG	CCDP given we are have chosen HS and 2 DGs are available	1e-5
CCDPNC0DG	CCDP given we are have chosen NC and no DGs are available	1e-1
CCDPNC1DG	CCDP given we are have chosen NC and 1 DGs is available	5e-3
CCDPNC2DG	CCDP given we are have chosen NC and 2 DGs are available	5e-5
CCDPNCrec	CCDP given we are have chosen NC and off-site power is recovered	5e-5
p1DGdown1	Probability that 1 DG is down between T1 and T2	2e-2
p_bothDGdown1	Probability that both DG are down between T1 and T2	1e-3
p_no_rec2	Probability that off-site power is not recovered after time 2	0.9
p_recovery1	Probability that off-site power recovered after between T1 and T2	0.5
p_unav1DG2_0DGav1	Probability that 1 DG is unavailable after T2 given that no DG were available between	2e-1
p_unav1DG2_1DGav1	Probability that 1 DG is unavailable after T2 given that one DG was available between	5e-2
p_unav1DG2_av1	Probability that 1 DG is unavailable after T2 given 2 DGs available between T1 and	2e-2
p_unav2DG2_0DGav1	Probability 2 DG unavailable after T2 given 0 DGs available between T1 and T2	0.5
p_unav2DG2_1DGav1	Probability 2 DG unavailable after T2 given 1 DGs available between T1 and T2	1e-2
p_unav2DG2_av1	Probability 2 DG unavailable after T2 given 2 DGs available between T1 and T2	5e-3

4.3.5: Best Strategy Evaluation: Expected Value results based on point estimates

After we have developed the ID or DT for our problem, we are able to evaluate the best outcome from an expected value point of view. Each decision alternative consists of a set of random event and outcomes. To each random event we have associated a probability (point estimate value) and to each outcome we have associated a preference value based on our Utility Function U, defined in (1).

The expected value of each decision alternative (say aj) is, in general, given by the sum of the products of the probability of each outcome multiplied by its Utility Function value:

$$E[aj] = \sum_{ij} p_{ij} U_{ij} \quad (2)$$

That is, for alternative j outcome i will have a probability p_{ij}. In particular p_{ij} is the probability of the path that leads to that outcome. In our case p_{ij} is calculated as a product of point estimates, and it is in its turn a point estimate. In our problem the best outcome will be the one that minimizes our losses, and hence the one that has the lowest value for E[aj].

The calculations based on point estimates for the probabilities lead to the following result (Table 13). The best decision at time T1 would be to go to hot shutdown. At time T2, in case we would have recovered off-site power, the best decision would be to go back to power. If, on the other hand, off-site power is not restored, the best outcome would be to go to cold shutdown.

Table 13: EV results

Decision 1	EV	Off-Site _Power	Decision 2	EV
Hot Shutdown	158	Yes	Back to Power	118
		No	Cold Shutdown	205 210 652

EV = Expected Value

4.3.6: Sensitivity and Uncertainty analysis

The previous results are based, as we said, on the expected value or on a point estimate of the probabilities. Theoretically, a point estimate or expected value of a probability is the number that better reflects our degree of belief of the likelihood of a certain event. However, in general, in very few situations the analyst has enough data to be one hundred percent confident that these values are the “true values”. Therefore, it is necessary to consider uncertainty on the parameters and compare the results of our uncertainty analysis with the results we obtained with the point estimate evaluation. To accomplish this task, we performed two types of analysis: a sensitivity analysis and a Monte Carlo uncertainty analysis.

4.3.7: Sensitivity Analysis (SA): Tornado Diagram and One Way sensitivity

Sensitivity analysis in a decision-making problem has the general scope of determining the most influential input parameter on the ranking of alternatives and, more in general, on the model.

The use of SA is twofold: first of all, SA results can be used as a check of the quality of the model. SA is precious in the corroboration of the model, since it is able to reveal eventual weakness and incoherent reasoning in the modeling process - as an example, let us thin of the case in which variables which should not play a role emerge as the most relevant. The second use is the following: once the Decision-Maker knows the relevant parameters (for example the probability that operators will perform correctly) he could take additional measures to increase or decrease the value of these parameters (additional training, for example), to increase the overall success probability of the strategy.

When using results derived from any SA method, the Decision-Maker should be aware of both its capabilities and limitations. In the remaining of this section we will comment on the results, insights and limitations connected with the use of Tornado diagrams and One Way SA, two techniques that have the advantage of being computationally simple.

The first SA technique we used is the so-called Tornado Diagram (Figure 17). Conceptually this technique tries to answer the following question: since we are not sure on the value of a certain parameter, which hence has a certain range of variation, what happens to the output when the parameter varies form its lowest to its highest possible value?

This technique consists in setting the input parameter to its lowest and to its highest value and collecting the output (expected value) values. The horizontal bars display the variation of the output relative to the variation of the input parameter. The larger the horizontal bars, the more relevant the parameter.

In our case, from Figure 17 we can say that the most influential variable on the best outcome of the decision (namely HS) is p_unav2DG2_av1 with interval of variation 0,0005 to 0,05. Variables like p_recovery1, CCDP1Bprec,CCDP1Bprec,CCDPHS0DG, p_unav1DG2, CCDPHS1DG, p_no_rec2, CCDP1rec, CCDPHS2DG, p_bothDGdown1, p_unav2DG2_1DGav1 have almost the same influence of the variation of the outcome, and all the other variables are less relevant.

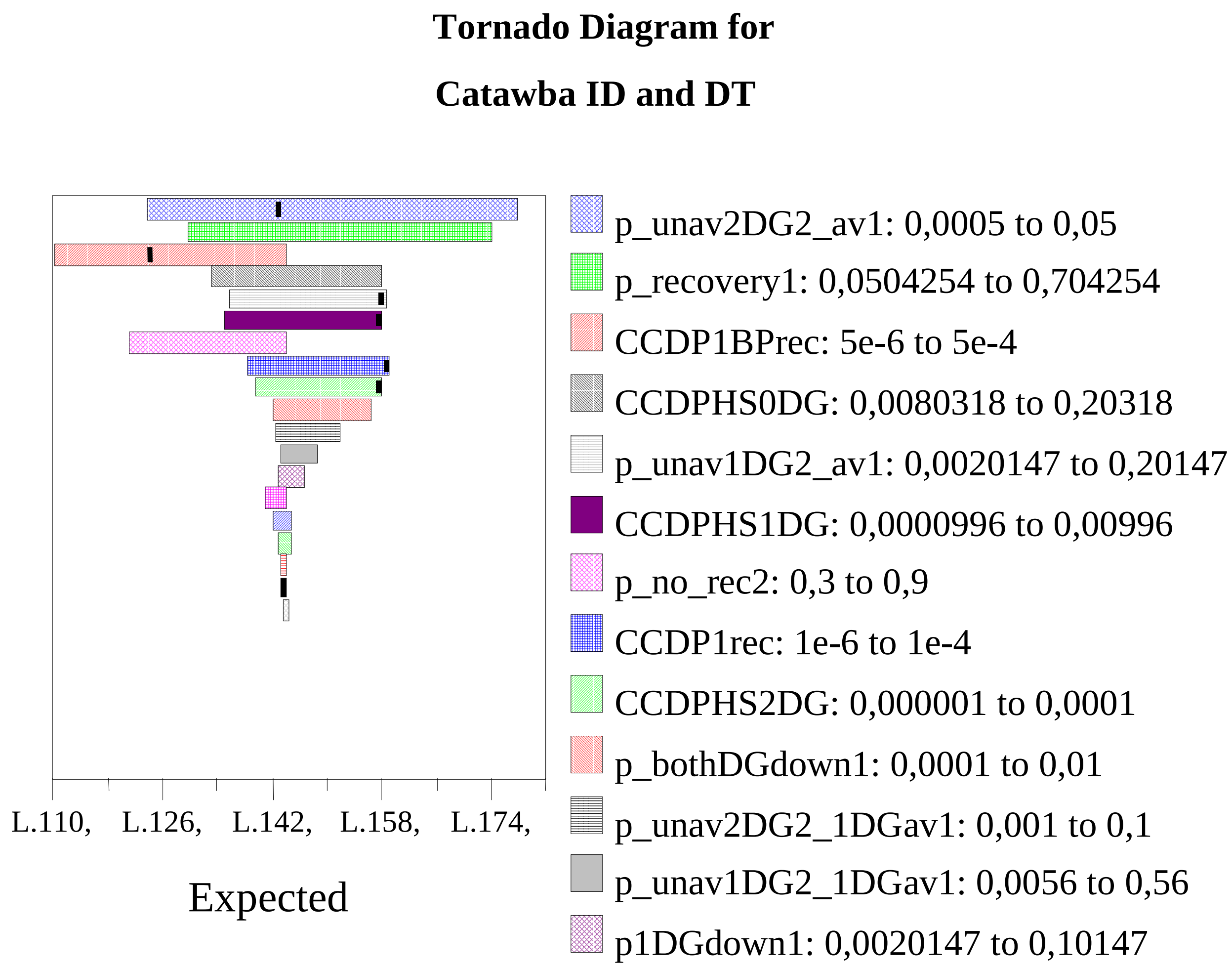


Figure 17: Tornado Diagram for Catawba ID and DT.

Let us now come back to our model, with the purpose of answering the following question: given that p_unav2DG2_av1 is the most influential variable, if we let it vary on its expected range, will the ranking of the output change? That is, if p_unav2DG2_av1 assumes a certain value, is it possible that HS is no more the best alternative?

This result can be obtained by the so called “One Way sensitivity Analysis” (see Figure 18).

This kind of analysis consists of varying the parameter of interest in its expected range and correspondingly plotting the decision alternatives. Figure 18 tells us, that, in our case, there is no reversal of the decision, since HS always is always the alternative with the least expected value.

In any case these results should be taken as an indication and not as an absolute information. In fact, considering the smallest and largest value of the parameter is not a complete information, since we are neglecting its distribution. That is, a parameter could have a large range of variation, but a very low probability of takes the extreme values. On the other hand, a parameter with a smaller range could have a higher probability of being at its extreme values. In other words, setting parameters at their extreme values, we are assuming uniform distributions for all of them. Another limitation arises from the fact that we are varying only one parameter at a time independently of all the others, while keeping the other fixed.

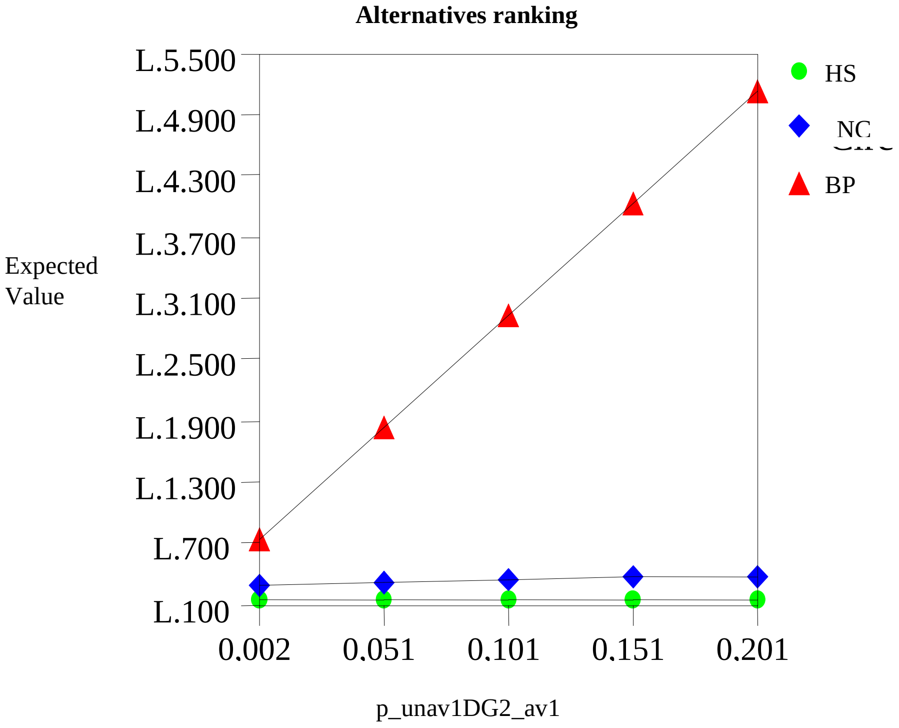


Figure 18: Alternatives ranking as a function of p_unav1DG2_av1

4.3.8: Monte Carlo Uncertainty Analysis

As mentioned before, the lack of knowledge on the values of parameters in the model leaves us not completely satisfied with simple point estimates results. To display our uncertainty on the parameters, the simplest way is that of assigning to each parameter a corresponding distribution. The distribution can be based on data or on judgment. Our model is now characterized by a set of parameters each associated with a certain distribution. In other words, each parameter is now a random variable. Suppose we run one MC story sampling all the parameters once. If we now calculate the expected value of the decision alternatives, we are able to know what is the best outcome given that the parameters assume the value of the sample. Suppose now we run another MC calculation with another sample. The best outcome could have changed.

If we now repeat the operation 1000 times, we can collect the result of each MC iteration and count the number of times each decision alternative is the preferred. Let us refer now to the Catawba example and in particular to Figure 19. The result is the, in 60% of the cases the best outcome of the first decision would have been HS, around 40% of the times would have been NC and in none of the MC trials BP would have been the preferred alternative.

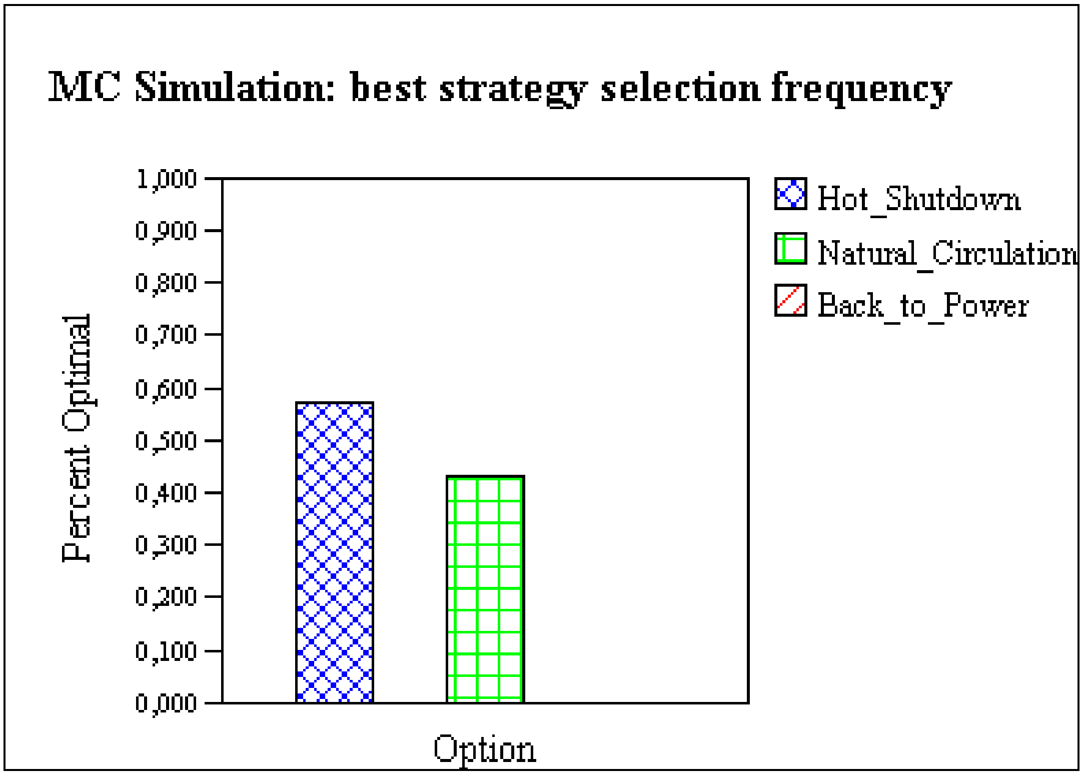


Figure 19: MC best strategy selection frequency for the first decision

For the second decision (Figure 20), in case off- site power is recovered, we would get that almost 80% of the MC stories led to BP as the preferred alternative.

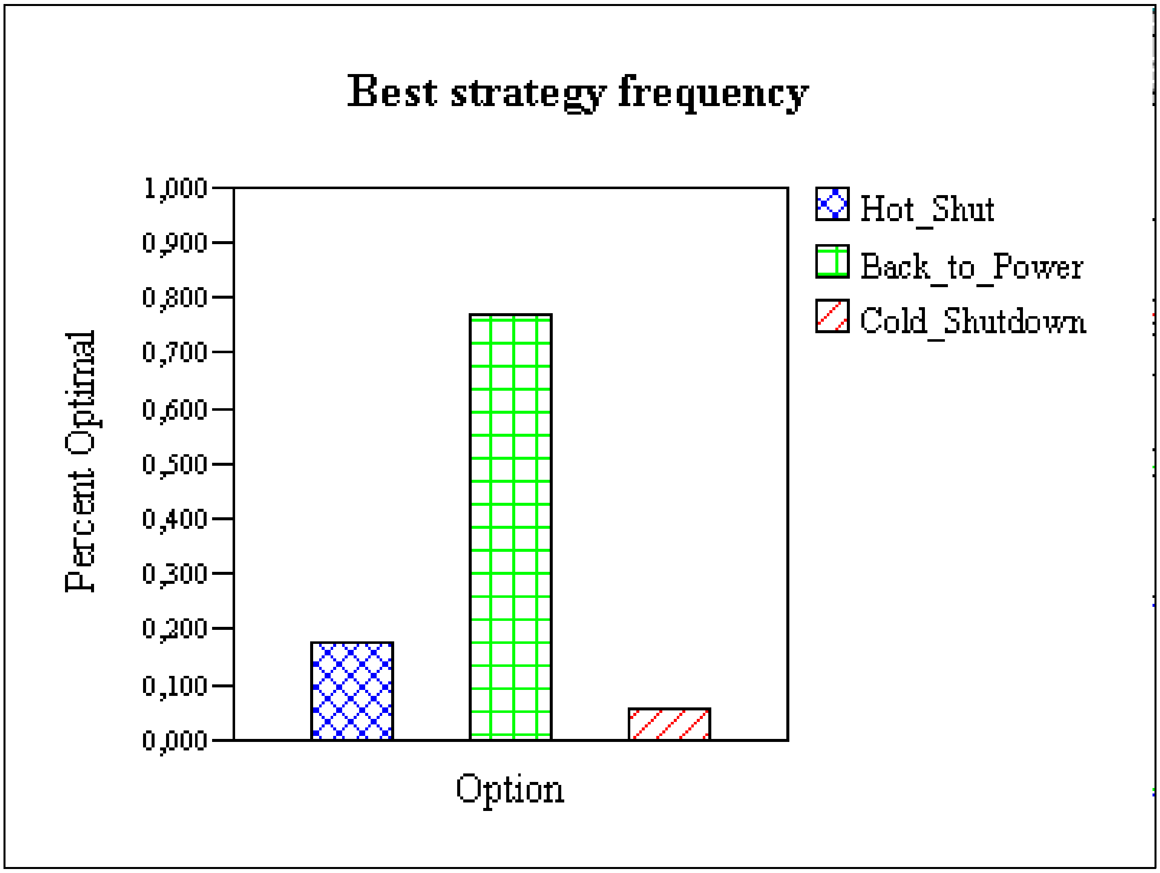


Figure 20: MC best strategy selection frequency for the second decision

The information we can draw from these graphs is a quantification of how uncertain we are on what is the best outcome. For example, Figure 19 tells us that for sure we would never have BP as best alternative in the first decision, but HS is not strictly dominant over NC. On the other hand, Figure 20 tells us that BP is dominant over the other alternatives, although all three of them are possible.

4.4. Conclusions about the decision-making aspects of the two case studies

In the above sections we have seen how insights drawn from PSA analysis enable us to:

S Represent the main decisions taken in an accident sequence

S Identify decision alternatives

S Individuate key elements (systems and dependencies) of the sequence

Once these have been identified, our knowledge of the timing of the sequence has enabled us to set the decision points in a time dependent flow. Representing the sequence as a generalized ID or DT, and assigning values to the probabilities of the events is the next logical step towards the evaluation of the decisions alternatives

From the Decision-Making point of view, the main differences between the Catawba event and the Davis Besse are:

S *Timing*: The time sequence of the events and the time interval between the decisions is in the order of minutes for the Davis-Besse event and of many hours for the Catawba Event.

S *Decision Makers*: In the first case, possibly due to the short duration of the event, no Emergency Centers were actuated. In this second case, on-site emergency centers were actuated, thus raising the issue of multiple decision makers and team structure in accident management.

The analysis of the second phase of the Catawba event has led us into the modeling of a decision problem rather different than the accident management situation described in the Davis-Besse event. While in the former case the focus fell on operator actions and possible mitigating strategies, in this later case, the focus is shifted towards the realm of operational/managerial decisions. While analyzing the event, besides deriving numerical information about the decision-making problem, we also derived some conclusions and insights about the steps of a top down methodological approach. The methodology will enable the analyst to integrate PSA aspects into operational decision-making, while casting operational decisions for NPPs in a decision-theoretical framework. Further refinement of the methodology and its corroboration will be part of the second phase of this project. For the moment, we limit ourselves to briefly discuss some of open issues that the methodological steps should be able to resolve.

Table 14: Methodological steps

Methodological steps
Alternatives Identification
Decisions Timing Identification
Configuration Individuation
Components Prioritization
From PSA to CCDP
Consequences Determination
Objectives Identification
Create ID or DT
Sensitivity and MC Analysis
Best Strategy Identification

The first issue regards time dependence in decision-making. PSA and decision trees offer respectively, a static representation of the plant accident sequences and of the decision-making problem. When the decision-maker is planning a strategy, how far in time to reevaluate a decision or to take certain actions could be a relevant element. In the Catawba event we solved the problem using the times in which the decisions were actually taken, while in a predictive mode, optimization of the time (as well as of the decision) could have a relevant role.

A second issue is represented by the formulation of complete evaluation criteria for the decision-making problem at hand. In a typical situation, consequences could range from radiation release, to economic loss and loss of prestige (e.g., Table 11). That is, in general we are dealing with decisions with multiple objectives and attributes. The task of formulating general evaluation criteria will be part of the second phase of this project.

A third issue is represented by the use of importance measures and sensitivity analysis techniques as a source of additional information for the Decision-Maker. As pointed out before, the “perfect technique” does not exist and the decision-maker must be aware of the capabilities and limitations of the SA technique he is using. Uncertainty analysis could also be improved by the use of other SA techniques recently developed in the sensitivity analysis field (Homma and Saltelli, 1996).

5. CONCLUSIONS AND RECOMMENDATIONS

This report summarizes the results of Task 2 of the project "The use of PSA to support Accident Management in NPPS".

The scope of Task 2 was to analyze in detail two "precursor events" in order to identify issues arising when PSA and formal decision-making techniques are used for incident management and operational decision-making. Two case studies, the Davis-Besse loss of main feedwater event and the Catawba loss of offsite power event, have been analyzed.

The starting point of the analysis was a description of the two actual incidents. This description was given in Section 2. The two incidents differed in the overall duration of each event. This time difference required decisions with variations in their characteristics. For example, the decisions during the David-Besse event involved extreme time pressures (due to lack of time) and were very critical (the event could have easily led to core damage). Conversely, during the Catawba event, a longer time and less critical decisions resulted in fewer and less demanding decisions. The Catawba event did not reach a critical point like the Davis-Besse incident, even though emergency centers were actuated. Also, in the Catawba event, the point of operational decision-making was at issue.

In Section 3 of the report, we focused on the PSA capability of modeling an incident. In so doing, we noted several items that both served to assist the decision-making process and complicated the overall analysis. First, we summarize the PSA assistance to the decision-making process:

S The PSA appears to be well suited for determining alternative operational decisions. These should be evaluated in a formal decision-making framework.

S The PSA appears to be well suited for indicating when, in a sequence of unfavorable events, critical decisions must be made.

S The ranking of components via the PSA appears to yield useful information on howthe importance of particular components varies as a function of time. This varying “importance” of components should be vital information to the decision-maker, since it may provide guidance as to where and how to focus resources.

S The PSA provides a formal structure for the evaluation of plant state uncertainties.

As mentioned above, we faced several issues that complicated the PSA analysis for use in incident management. These issues are summarized below:

S The treatment of basic events in the PSA model during the time of an incident is a *critical* issue.

- We noted that there were two ways to represent a failed component. Depending on which one is used, we may impact the quality of the final PSA results may be important.

- We noted that for redundant components, adjustments to individual basic events must also be reflected on the associated common-cause event failure the two basic events are inter-related.

- Maintenance outages for all components probably should be modeled as a known boundary condition of the state of the plant.

- The human failure probabilities relevant to a particular plant state may require that nominal basic event probabilities be adjusted to reflect performance factors (e.g., short time, unfamiliar task) during an incident.

S The utilization of traditional PSA importance measures is another *critical* issue. There are questions as to the overall applicability of traditional importance measures. In addition, reliance on a numerical *change* in an importance measures (e.g., as a function of time or configuration) is an untested and untried methodology.

S Issues of timing during an incident are important to both the PSA and the decision-making methods. Times to perform certain actions (as dictated by the PSA and decision criteria) are required information in order to determine adequacy of such decisions.

S Aspects of "going back" and moving to "OK" sequences on an event tree are ways to avert core damage situations. Normally, the PSA only provided failure cut sets for the "not OK" sequences. Attempting to solve the "OK" sequences complicated the analysis process and, again, was an untested and untried methodology.

In Section 4, we analyzed and proposed a way to cast the PSA approach in a decision-making framework. As can be seen from the conclusions of the Task 1 report and from the analysis performed for the two case studies, accident management must be considered a sequential decisions problem. We know that decisions are not explicitly represented in PSA. Consequently, we must determine whether PSA is capable of supporting the main decisions in an incident management strategy. The results of our analysis (see Section 3.1, Figure 1) are encouraging. It does appear that PSA is capable of providing decision alternatives, alternatives that feed directly into the formal decision-making techniques presented in Section 4.

Furthermore, it can be seen from our analysis that PSA information can be successfully used to establish the relevant dependencies between decisions, the plant states, and actions carried out during an incident. This information can be cast in a Decision Tree (DT) or Influence Diagram (ID) representation. Integrating the traditional PSA event tree approach with the decision-making aspects naturally leads to the extensions of the usual PSA event trees (where bifurcation is determined only by random events) to DTs, where bifurcation is not only determined by chance events, but also by actual decisions. DTs are sometimes complicated to read, especially in the presence of a large number of branches. In this situation, the DT can be complemented by the use of IDs. IDs can offer a more compact and high-level representation of the problem. As we have explained in Section 4, IDs and DTs are two ways of expressing the same model of the accident sequence. The nodes that characterize these diagrams will reflect the dependencies established through PSA analysis. The results of our analyses allow us to conclude that PSA coupled with IDs and DTs can be used successfully to model operational-managerial decisions as well as decisions, events, and dependencies during off-normal situations.

In summary, the analysis of the two case studies has provided a fruitful arena for exploring the integration of PSA and time-dependent DTs and IDs. This type of blended approach would be capable of accounting for

S Sequential decisions in time

S Event dependencies

S Decision-maker values

S Critical junctions during an incident

S Relevance of plant components or systems.

Thus, it is believed that this methodology is superior to an analysis that is based solely on physical aspects of the situation or on simple engineering judgment. But, further research, on several aspects of the proposed methods, is required. In addition to these areas of research, the particular mode of operation for the advisory system may require special investigation. When moving from a retrospective analysis where we know what happened (i.e., historical) to a predictive one, new issues will arise. These issues include:

S The identification of the critical decisions

S The prediction of the time interval between the beginning of various decisions and events to a postulated undesirable event (e.g., core damage)

S The presence of emergency centers and communication between such entities

S The integration of human reliability aspects, notably during the execution of important tasks;

S The control and flow of information for the advisory system

S The response time for an incident management system.

This issues and results identified in this report will be addressed the Phase 2 follow-up research to be performed. It is anticipated that at the conclusion of that research, a prototype advisory system will be realized.

6. REFERENCES

ACRS, Report dated October 12, 1999 from D.A. Powers, Chairman, ACRS, to Greta Joy Dicus, Chairman, NRC, Subject: Proposed Plans for Developing Risk-Informed Revisions to 10 CFR Part 50, Domestic Licensing of Production and Utilization Facilities.

Bertucio, R. C. and J. A. Julius, *Analysis of Core Damage Frequency: Surry, Unit 1 Internal Events,* NUREG/CR-4550, SAND86-2084, Volume 3, Revision 1, Parts 1 and 2, April 1990.

Catton, I .and Kastenberg, W.E, *Reactor Cavity Flooding as an Accident Management Strategy,* Reliability Engineering and System Safety, 62:59-70, 1998.

Cheok, M.C., G.W. Parry, and R.R. Sherry, *Use of importance measures in risk-informed regulatory applications*, Reliability Engineering and System Safety **60**, 213-226, 1998.

Dougherty, E. M., *Credibility and Uncertainty Associated with Accident Management Actions*, Reliability Engineering and System Safety, 37, 1992, 45-55.

Fleming, K. N., *Developing Useful Insights and Avoiding Misleading Conclusions from Risk Importance Measures in PSA Applications*, PSA '96, Park City, Utah, Sept. 29 - Oct. 3, 1996, American Nuclear Society.

Holmberg, J., Hukki, K., Norros, L., Pulkkinen, U., Pyy, P., *An integrated approach to human reliability analysis - decision analytic dynamic reliability mode,* Reliability Engineering and System Safety, **65**, 239-250, 1999

Homma, T., Saltelli, A. *Importance Measures in global Senstivity Analysis of non-linear models,* Reliability Engineering and System Safety, **52**, 1-17, 1996

Jae, M., Apostolakis, G., *The Use of Influence Diagrams for Evaluating Severe Accident Management Strategies*, Nuclear Technology, 99:142-157, 1992.

Jae, M., Milici, A., Kastenberg, W., and G. Apostolakis, *Sensitivity and Uncertainty Analysis of Accident Management Strategies involving Multiple Decisions,* Nuclear Technology, 104: 13-36, 1993.

Nuclear Regulatory Commission, *Loss of Main and Auxiliary Feedwater Event at the Davis-Besse Plant on June 9, 1985,* NRC Report NUREG-1154, July 1985.

Smith,C.L., Borgonovo, E., Apostolakis, G.E.: *Review of International Activities in Accident Management and Decision Making in the Nuclear Industry*, Task1 Report, Internal Communication, 1999

Smith, C.L., T. A. Thatcher, and J. K. Knudsen, 1998. *Systems Analysis Programs for Hands-On Integrated Reliability Evaluations (SAPHIRE) Basic Training Course and SAPHIRE Basics Workshop Manual*, INEEL/EXT-1998-1136.

Smith, C. L., *Calculating Conditional Core Damage Probabilities for Nuclear Power Plant Operations* Reliability Engineering and System Safety, **59** (1998) 299-307.

O. Svenson, *A Decision Theoretic Approach to an Accident Sequence: When Feedwater and Auxiliary Feedwater Fail in a Nuclear Power Plant*, Reliability Engineering and System Safety, 59, 243-252, 1998.

Vesely, W.E., *Reservations on 'ASME Risk-Based Inservice Inspection and Testing: An Outlook to the Future*, Risk Analysis 18, 423-425, 1998.

APPENDIX A

Excerpts from the LER for the Catawba Loss of Offsite Power Incident

FACILITY NAME: Catawba Nuclear Station
DOCKET NUMBER: 05000414
TITLE: LOSS OF OFFSITE POWER DUE TO ELECTRICAL COMPONENT FAILURES
EVENT DATE: 02/06/96 LER #: 96-001-00

ABSTRACT:

Unit Status: Unit 2 - Mode 1 (Power Operation) at 100 percent power.
Event Description: On February 6, 1996, at 1231 hours, ground faults on the resistor bushings for 2A Main transformer X phase potential transformer and 2B Main Transformer Z phase potential transformer resulted in a phase to phase fault. Protective relay actuation on both Main Transformers resulted in a loss of offsite power. The reactor tripped on Reactor Coolant Pump bus underfrequency. As a result of the blackout, 2A Emergency Diesel Generator started and sequenced on all required loads. 2B Emergency Diesel Generator was inoperable due to battery charger repairs, therefore B Train 4Kv Essential Bus did not automatically reenergize. Cold auxiliary feedwater being supplied to the steam generators, in combination with the effects of various steam loads, resulted in a Low Steamline Pressure Safety Injection. At 1522 hours, B Train 4Kv Essential Bus was energized from 2B Emergency Diesel Generator. By 2000 hours, both 4Kv Essential Buses were being supplied from train related offsite power sources.

EVENT DESCRIPTION

February 6, 1996

1230:49 Hours X phase potential transformer for 2A Main Transformer shorts to ground. Z phase potential transformer for 2B Main Transformer shorts to ground. Phase to phase ground actuates protective relaying for 2A and 2B Main Transformers. All AC power is lost. The reactor trips on 2 out-of 4-Underfrequency - NC Pumps. Turbine trips on reactor trip.

1230:57 Hours Undervoltage on 4Kv Essential Busses 2ETA and 2ETB initiates auto-start to D/G 2A and 2B. Turbine Driven Emergency Feedwater Pump (TDCAP)starts. 2A D/G auto-starts as required. 2B D/G is inoperable due to battery charger work in progress.

1230:58 Hours 2A D/G reenergizes 4Kv Essential Bus 2ETA. Blackout loads begin sequencing on as expected.

1231:04 Hours 2A S/G is being supplied 2A MDCAP. 2B S/G is being supplied from both 2B MDCAP and the TDCAP.2B S/G is being supplied from the TDCAP. 2D S/G is not being supplied from any source. 2A, 2B, 2C and 2D S/G pressures begin to decrease.

1231:19 Hours All blackout load groups for 2ETA are energized as expected.

1232:45 Hours CF Isolation occurs as expected on Reactor Trip with Low Tave. Manual MSIV closure was initiated as directed by the 1236 Hours Emergency Procedure in effect.

1238:28 Hours SI automatically initiates on Low Steam Line Pressure in 2A S/G. Auto sequencing begins loading LOCA loads on 4Kv Essential Bus 2ETA. 4Kv Essential Bus 2-ETB remains without power.

1238:50 Hours All LOCA load groups for 2ETA are energized as expected.

1243 Hours A Notification Of Unusual Event (NOUE is declared in accordance with the site Emergency Plan for LOSS OF POWER

1247 Hours Pressurizer Power Operated Relief Valve (PORV) 2NC34A begins to cycle periodically as expected to limit NCS pressure.

1257 Hours Notification is sent to activate the Technical Support Center (TSC) and the Operational Support Center (OSC).

1300 Hours Criteria is met for SI termination.

1307 Hours ECCS flow to the NCS is terminated.

1310 Hours PZR level is off scale high. The NCS is water solid.

1320 Hours PRT pressure increases. The PRT rupture disc "blows" as expected as 2NC34A continues to cycle, limiting NCS pressure. 1339 Hours The TSC and OSC are activated.

1357 Hours Normal NCS letdown is established.

1522 Hours 4Kv Essential Bus 2ETB is energized from 2B D/G.

1800 Hours 4Kv Essential Bus 2ETB source is transferred from 213 D/G to transformer SATB, which is being powered from a unit1 B Train offsite power source.

1810 Hours 2B D/G is secured.

1926 Hours A steam bubble is formed in the pressurizer.

2000 Hours 4Kv Essential Bus 2ETA source is transferred from 2A D/G to transformer SATA, which is being powered from a unit 1 A Train offsite power source.

2117 Hours Automatic SI initiation logic is reestablished.

2125 Hours Natural Circulation cooldown is initiated.

February 7, 1996

0445 Hours Unit 2 enters Mode 4, Hot Shutdown.

1702 Hours Unit 2 enters Mode 5, Cold Shutdown. T.S. 3.6.1.4 Action for Containment Pressure is exited.

February 8, 1996

0120 Hours Main Transformer 2B is reenergized from offsite via the 230KV switchyard.

0215 Hours The site exits the Emergency Plan for LOSS OF POWER and terminates the NOUE.

APPENDIX B

Sensitivity Analyses for the Davis-Besse Incident

Sensitivity Analysis for the ID-DT of the Davis-Besse event

Another of the potentialities of the methodology we are proposing is the analysis of the important parameters and variables in the accident sequence (Sensitivity Analysis). The immediate result of this analysis is a corroboration of our model: if variables which should not play a role in our model, are important, is a signal of some inconsistency in our model: something is missing or not adequately modeled in our analysis.

Once we have verified that our analysis is correct, the ordering of the variables would give us the sensible parameters of the model: for example, suppose that the probability of no error in starting AFW manually is important for the sequence. One message could be that we have to train the operators particularly on that point in order to avoid bad consequences during the sequence.

Here we give here the results of sensitivity analysis performed for the Davis-Besse event, as an illustration.

The list of variables is given in table B1.

Figure B.1 represents a "Tornado Diagram" for the Davis-Besse simplified ID of figure 4.5. The variables are ranked in terms of the variation of the outcome compared to the variation f their input value. We see that the first 7 variables are far more important than the others. Notably we have: the probability of error at 9 minutes while trying to restore auxiliary feedwater (pe9w), the probability of causing core damage while performing Feed and Bleed (PcdFeBe and PcdFeBne) and the probability that AFW is available between 6 and 9 minutes. The message is clear: AFW is the critical system in our sequence and the probability of correctly performing F&B plays an important role in the decision. We could believe that going to F&B is a more conservative action, but this is not the case if there is a high probability of error or not performing it successfully.

The information figure B.2 gives us is the following: we left the values of the variables pe9F&B (probability of operator error while performing feed and bleed) and pe9w (probability of operator error while trying to restore AFW after 9 minutes) vary from 0 to 1 (the whole range). The green area in the diagram represents the combination of values of pe9w and pe9FeB for which to go to FeB is the best decision. For example, let us take point (0.5, 0.5): it follows in the green zone: this means (see the legend on the right of the diagram) that going to F&B would be the best decision. We can see that for almost every pair if values, the best decision would be to go to feed and bleed, and only in cases of high probability of error while performing F&B and low probability of error while trying to restore AFW, "Wait for restoration of AFW" would be the best alternative.

Table B.1: List of variables for the Davis-Besse ID-DT

Name
Pawa6e
Pawa6ne
Pawa9ea
Pawa9ne
Pawa9nea
Pawa9neu
Pcdafwav9e
Pcdafwav9ne
Pcdafwunav9e
Pcdawa9e
Pcdawa9ne
Pcdawu9e
Pcdawu9ne
PcdFeBe
PcdFeBne
Pdiag
Pe9FeB
Pe9w
Peaw6
Pew6

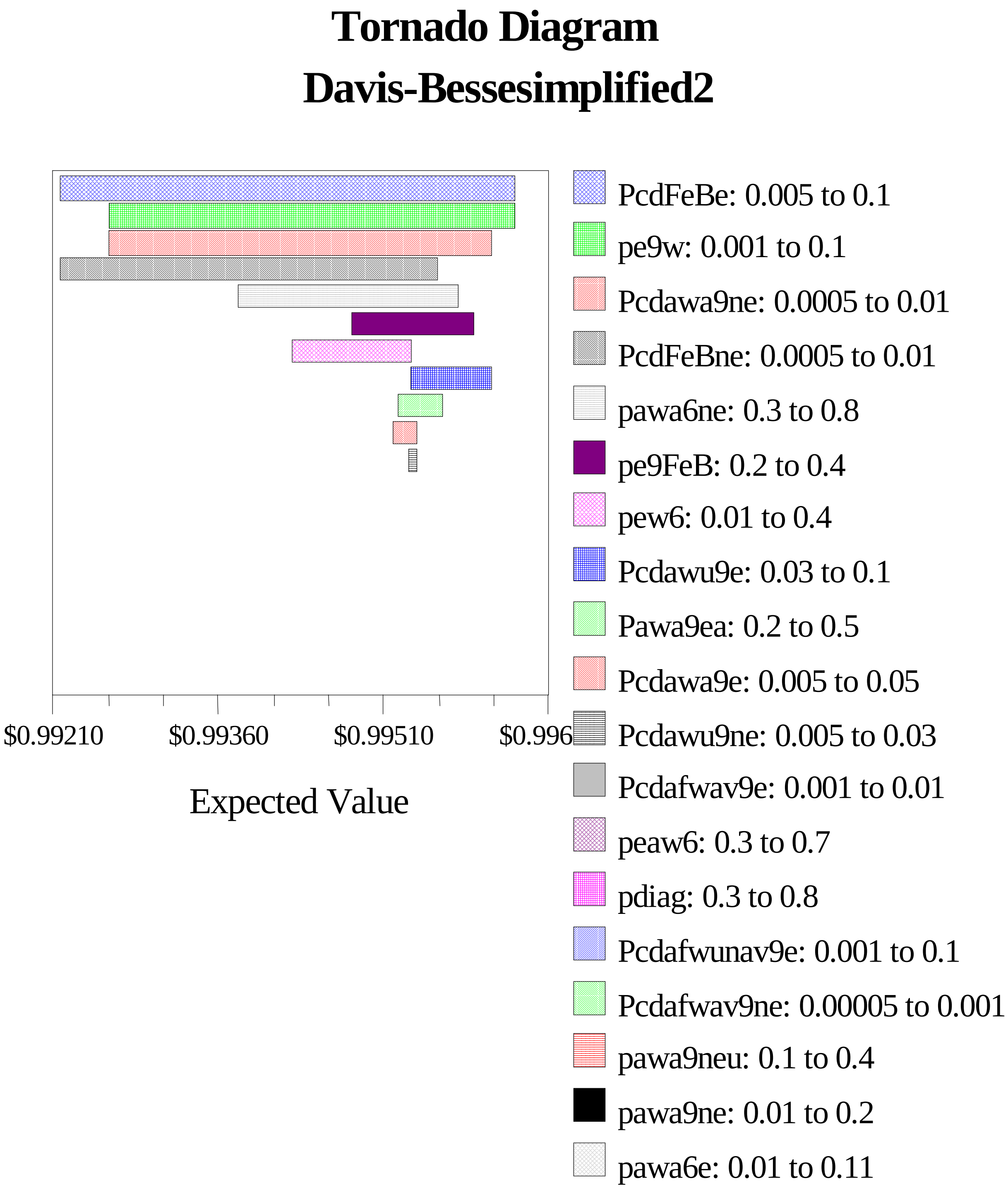


Figure B.1. Tornado Diagram for the Davis-Besse simplified ID-DT of figure 12, 13 and 14

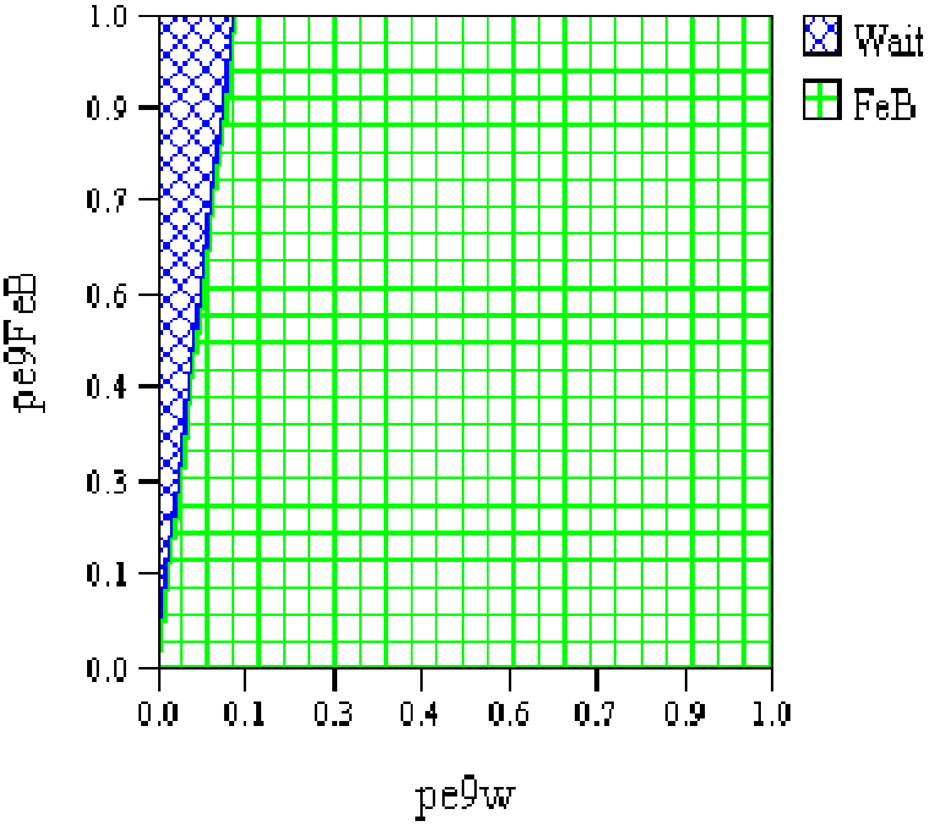


Figure B.2. Two way sensitivity analysis for the decision at t= 9 min for the Davis Besse event.

For the sensitivity analysis described in this Appendix, used the ID represented in Figure B.3, instead of that in Figure11. We used this ID for a simple reason; the ID of figure 11 was developed for an illustrative purpose, in order to show to the reader how to model the main decisions, and much of the information displayed is redundant. Therefore the analyst can come to a more compact representation of the problem, and that is what we have in the ID of figure B.3[1].

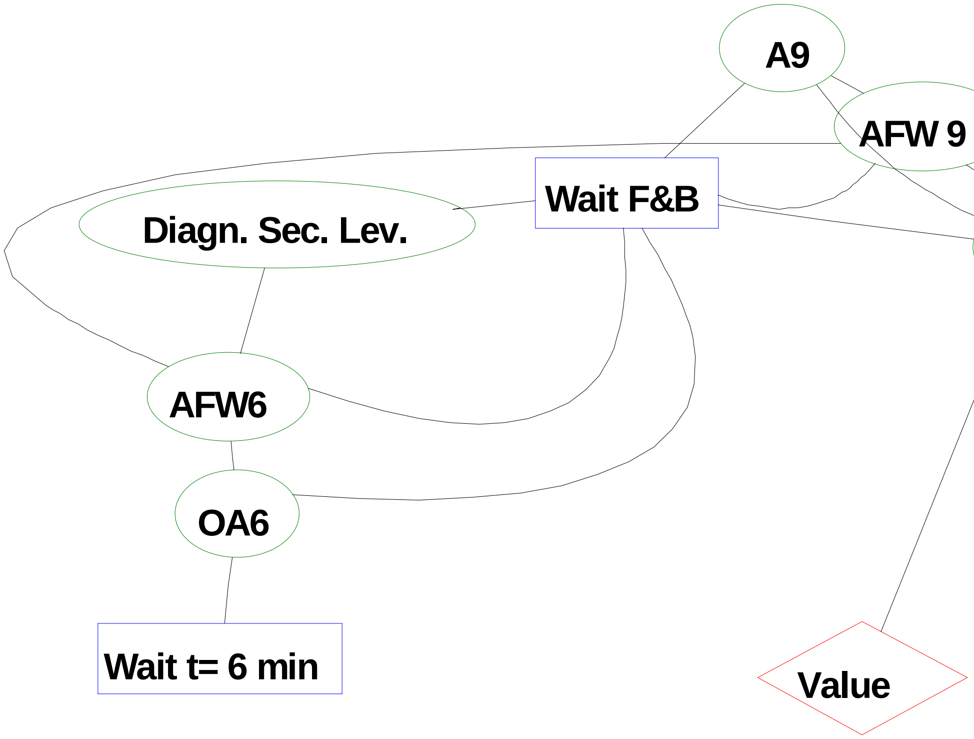


Figure B.3. More compact Influence diagram for the Davis-Besse event

[1] It is only a technical detail how to pass from one ID to the other, and for the moment we will not go further into the analysis. The purpose of the discussion here is to give a sense of the method for modeling off-normal decisions.